THE DEPARTMENT OF JUSTICE'S "OPERATION CHOKE POINT"

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JULY 15, 2014

Printed for the use of the Committee on Financial Services

Serial No. 113–90

U.S. GOVERNMENT PUBLISHING OFFICE

91–154 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

GARY G. MILLER, California, *Vice Chairman*
SPENCER BACHUS, Alabama, *Chairman Emeritus*
PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
SHELLEY MOORE CAPITO, West Virginia
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
PATRICK T. MCHENRY, North Carolina
JOHN CAMPBELL, California
MICHELE BACHMANN, Minnesota
KEVIN McCARTHY, California
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
ROBERT HURT, Virginia
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee
MARLIN A. STUTZMAN, Indiana
MICK MULVANEY, South Carolina
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
TOM COTTON, Arkansas
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana

MAXINE WATERS, California, *Ranking Member*
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
RUBÉN HINOJOSA, Texas
WM. LACY CLAY, Missouri
CAROLYN MCCARTHY, New York
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
GARY C. PETERS, Michigan
JOHN C. CARNEY, JR., Delaware
TERRI A. SEWELL, Alabama
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
PATRICK MURPHY, Florida
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
STEVEN HORSFORD, Nevada

SHANNON MCGAHN, *Staff Director*
JAMES H. CLINGER, *Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

PATRICK T. MCHENRY, North Carolina, *Chairman*

MICHAEL G. FITZPATRICK, Pennsylvania, *Vice Chairman*
SPENCER BACHUS, Alabama
PETER T. KING, New York
MICHELE BACHMANN, Minnesota
SEAN P. DUFFY, Wisconsin
STEPHEN LEE FINCHER, Tennessee
RANDY HULTGREN, Illinois
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania

AL GREEN, Texas, *Ranking Member*
EMANUEL CLEAVER, Missouri
KEITH ELLISON, Minnesota
CAROLYN B. MALONEY, New York
JOHN K. DELANEY, Maryland
JOYCE BEATTY, Ohio
DENNY HECK, Washington
DANIEL T. KILDEE, Michigan
STEVEN HORSFORD, Nevada

CONTENTS

WITNESSES

TUESDAY, JULY 15, 2014

APPENDIX

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

THE DEPARTMENT OF JUSTICE'S "OPERATION CHOKE POINT"

Tuesday, July 15, 2014

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON OVERSIGHT
AND INVESTIGATIONS,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 10:03 a.m., in room 2128, Rayburn House Office Building, Hon. Patrick McHenry [chairman of the subcommittee] presiding.

Members present: Representatives McHenry, Fitzpatrick, Bachmann, Duffy, Fincher, Wagner, Barr; Green, Cleaver, Maloney, Delaney, Beatty, Heck, and Kildee.

Ex officio present: Representatives Hensarling and Waters.

Also present: Representatives Garrett and Luetkemeyer.

Chairman MCHENRY. The Subcommittee on Oversight and Investigations will come to order.

Without objection, the Chair is authorized to declare a recess of the subcommittee at any time. Also, without objection, members of the full Financial Services Committee who are not members of the Oversight and Investigations Subcommittee may participate in today's hearing for the purpose of making an opening statement and questioning the witnesses.

The title of today's subcommittee hearing is, "The Department of Justice's 'Operation Choke Point'." The Chair now recognizes himself for 5 minutes.

In the spring of 2013, the Department of Justice launched what is known as "Operation Choke Point," representing an expansive investigation of banks and payment processors with the objective of combating consumer fraud by choking out fraudsters' access to payment systems.

This committee values the Department's procedural methods of proficiency, identifying and prosecuting fraudsters. And it appreciates its effect on our economic prosperity, as well.

However, equally important to the Federal prosecution of alleged fraudsters are lawful methods by which the government and regulators identify and investigate those in question.

For any division of government to seemingly circumvent lawful, judicious means of conducting Federal investigations, it not only subjects itself to rigorous congressional oversight, but it also betrays those whom it seeks to protect. And that is the American people.

Directly contacted from enterprises and individuals, Congress has learned that after "Operation Choke Point's" onset, various lawful businesses were identified, and were notified that their bank accounts were being terminated.

When these legitimate enterprises inquired about this sudden termination of their accounts, their banks expressed that it was a result of "regulatory trends" or "heightened scrutiny," and explicitly denied any negative review of the account holder's financial risk.

Upon receiving copies of account termination letters from targeted merchants, Members of Congress questioned why banks had unexplainably used the cliched teenage break-up excuse, "It's not you, it's me."

In the last year, to comprehend how "Operation Choke Point's" targets were identified and how banks were getting mixed up, members of this Committee and of the Oversight and Government Reform Committee here in the House have written letters to regulators and requested documents from the Department of Justice.

From the committee's experience, the Department of Justice initially attempted to block congressional oversight and investigations of "Operation Choke Point." But the DOJ has since provided 854 pages of internal memoranda, e-mail communications, and presentations that have provided some detail of its investigation.

The initial findings are quite disturbing. Rather than directly investigate merchants for fraudulent activities, the Department of Justice subpoenaed banks and payment processors of targeted merchants to effectively compel them to choke off businesses from accessing the banking system.

Consequently it seems that "Operation Choke Point" may have led to banks terminating their relationship with unjustifiably named, "high-risk" merchants out of fear of civil and criminal liability from the Department and other financial regulators, as well.

Equally as troubling, "Operation Choke Point's" regulatory approach of employing an axe rather than a scalpel and informal operations suggests it, as another iteration of this Administration's game plan to circumvent the rule of law and Congress to achieve ideological objectives.

Even worse, the Department of Justice and the FDIC have blocked the committee from meaningfully understanding "Operation Choke Point" by failing to provide details about the program, and financial regulators have even misled this committee as to the breadth of their cooperation when engaging with banks.

Even with this much established, the irony is that the full role of financial regulators in "Operation Choke Point" remains a mystery. That is why we had this hearing today.

But then again, what a congressional inquiry has made clear is that this Administration and financial regulators have raised serious concerns of collaborated effort to facilitate an ideological crusade against industries profiled by the government through their abusive threat of launching Federal investigations.

This is not the intent of the rule of law in our system.

The Department of Justice may have originally advertised "Operation Choke Point" as an honorable, authentic investigation to combat consumer fraud.

Yet, unfortunately, congressional investigations have begun to uncover the questionable legal authority of "Operation Choke Point" inappropriately compelling banks to serve as the moral compass and law enforcement for our market economy.

This raises serious questions about the motives of and threats issued by the Department of Justice and financial regulators.

It is my hope that today's witnesses will assist this committee in better understanding the truth of "Operation Choke Point" by revealing the demonstrated actions of the Department of Justice and the FDIC to determine whether lawful businesses were indeed victims of an objectionable government operation.

I will now recognize the ranking member of the subcommittee, the gentleman from Texas, Mr. Green, for his opening statement.

Mr. GREEN. Thank you, Mr. Chairman.

I thank the staff for the outstanding job it has done in providing us with intelligence. I would like to also thank the witnesses for appearing today.

Mr. Chairman, we live in a world where financial and technological innovations present greater access and convenience for the American consumer. Unfortunately, this also provides the doer of fraudulent deeds greater opportunities to perpetrate crimes on consumers.

In 2013, the Automated Clearing House processed approximately 22 billion transactions worth about $37.8 trillion.

As innovative technologies evolve to benefit consumers, innovative methodologies must also evolve to protect consumers. Fraud detection and prevention methodologies are good for both consumers and businesses. Undetected fraud can bankrupt a consumer and put a business out of business.

Today, we will examine the relationship between banks, their business associates known as processors, and the consumers. And in so doing, I think it appropriate to use at least one very elementary example so as to give some clarity to persons who may be watching who are not familiar with this process.

Typically, with a simple example, we would find that a person sitting at home is approached by a business that would like to have that person make a purchase. Let's assume that this is a telemarketer. This telemarketer will present the consumer with a product.

If the consumer makes a purchase, that purchase is handled by a processor. A processor would be the company that works with the telemarketer. The processor receives the payment. The processor will then take the payment and deposit it in a bank. That bank then becomes the means by which the payments are paid to the telemarketer.

And once these payments are made, let's assume that the consumer concludes that there has been an overcharge. A chargeback can occur. The chargeback is called to the attention of the bank. The consumer gets redress.

The question becomes this: Is a bank required, or should a bank be required, to keep a record of chargebacks? And if the record of chargebacks is maintained, would one incident of a chargeback indicate anything more than a mistake? But if 10,000 chargebacks

occur, would that indicate activity? And if activity occurs, should activity be investigated?

And if activity is investigated and is found to be fraudulent, should the bank have some responsibility if it knew that the activity was occurring but did nothing?

There are serious questions to be answered. I believe we have capable, competent, qualified witnesses here today who can help us answer these questions. The question also occurs as to whether or not a bank has a duty to perform due diligence as it relates to the business associates it has who are doing business with other businesses.

And if it does have the requirement to perform due diligence, can that due diligence be outsourced to a processor who does business with a telemarketer? And if it is outsourced, are there consequences associated with it? What level of due diligence must the processor employ? Does it have the same level of due diligence placed upon it as the banks? And can a lack of due diligence by a processor in some way impact the liability of the bank with which it is doing business?

We really should take a close look at these questions, and we really should examine the difference between an incident and criminal activity. One occurrence, an incident; thousands of occurrences can be concluded to be activity. Should activity be investigated? And if so, should the banks provide intelligence such that the activity can be appropriately investigated?

Mr. Chairman, I look forward to hearing the answers to these and many other questions from the witnesses that we have today. And I will yield back the balance of my time.

Chairman MCHENRY. We will now recognize the gentleman from Missouri, Mr. Luetkemeyer, for 2 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman, for allowing me to participate today.

"Operation Choke Point" takes a new approach to banking supervision. If you don't like a given industry, bend your authorities and force that industry out of the financial services space, making it impossible for it to survive.

How does it work? DOJ staff who conceived of "Operation Choke Point" summed it up in a November 5, 2012, memo to Mr. Delery: "Banks are sensitive to the risk of civil and/or criminal liability and regulatory action." In other words, DOJ can intimidate banks into doing what it wants by threatening them with subpoenas including with the regulators.

Since last August, I have met with some of our regulators and even one of the witnesses on today's panel. In each of those meetings, the regulators agreed that casting a wide net and targeting legal industries is inappropriate. But despite that sentiment, "Operation Choke Point" continues.

I am troubled that requests I have made for cooperation over the past year have fallen on deaf ears. To that end, I have taken the step of trying to solve the problem by offering a bill, the "End Operation Choke Point Act," under which financial institutions will be granted the safe harbor necessary to serve legally operating customers—key words: legally operating customers.

Equally important, legislation will ensure that DOJ will not be able to act unilaterally in a broad-brush approach in attacking legal industries.

Mr. Chairman, I look forward to the discussion on what I find to be an indefensible and irresponsible approach to regulation.

I yield back.

Chairman MCHENRY. We will now recognize the gentlelady from Ohio, Mrs. Beatty, for 2 minutes.

Mrs. BEATTY. Thank you, Mr. Chairman, and Mr. Ranking Member. And thank you to our witnesses today. You have already heard definitions of "choke point." We have actually heard some "thank you's" to the Department. And then, we have heard the axe versus the scalpel.

Today, we look forward to hearing from you. And Mr. Chairman, I think this hearing is quite timely. We also know that we are on a parallel track with the House Judiciary Committee, which is also looking at this. While "Operation Choke Point" is a fairly recent undertaking, as you have heard, by the DOJ, designed to root out consumer fraud from the United States fiscal markets.

I think today in hearing from you, we need to determine, if we go back in history to when we heard we were "too-big-to-jail," if we should have done more to prosecute. And now we are hearing Administration or Department objectives are too over-zealous.

So, here is where I am in my opening remarks. Each year, consumers, banks, merchants and third-party payment processors conduct trillions of dollars of legitimate electronic transactions in a safe and efficient manner, maybe because oftentimes the DOJ has applied the scalpel to make sure that things are tweaked so we are able to protect our consumers.

Now, where I agree with the Act is that there are bad actors and they persist today. Unlicensed lenders make loans that violate State usury laws, or out-of-the-country Web sites may conduct unlawful online gambling rackets, just as an example. When banks or third-party payment processors facilitate automatic consumer bank withdrawals that enable unlawful activity to occur, it has a devastating impact on the lives of those consumers, our communities. And it also affects the good actors.

This hearing is supposed to evaluate "Operation Choke Point" with an eye towards ensuring that businesses operate lawfully and are not denied access to banking services.

Thank you, Mr. Chairman.

Chairman MCHENRY. We will now recognize our witnesses. Our first witness is Mr. Stuart Delery, who is the Assistant Attorney General for the Civil Division at the U.S. Department of Justice. He was sworn in as Assistant Attorney General on August 5, 2013. He has led the Division since March of 2012. As the Assistant Attorney General, Mr. Delery oversees the largest litigating division in the Department of Justice.

Mr. Delery joined the Department of Justice in January of 2009 as Chief of Staff and Counselor to the Deputy Assistant Attorney General. He later served as an Associate Deputy Attorney General. And prior to that, he served as Senior Counselor to the Attorney General.

Mr. Delery graduated from Yale Law School and the University of Virginia.

Our second witness is Mr. Richard Osterman, who is currently serving as the Acting General Counsel to the Federal Deposit Insurance Corporation. Mr. Osterman is the Deputy General Counsel for Litigation Resolution Branches in the Legal Division of the FDIC. The branch provides litigation counsel for the FDIC and comprehensive legal support for the FDIC's resolution receivership functions.

Mr. Osterman has served as Assistant General Counsel for the General Litigation Section, which includes appellate litigation and so on and so forth. And prior to that time, he was Assistant General Counsel for the receivership operations and the litigation sections, which, as we know, were very busy during that era.

He has a B.A. from Swarthmore College and a J.D. from the University of Baltimore School of Law.

Out third witness is Mr. Daniel Stipano, who is the Deputy Chief Counsel in the Office of the Comptroller of the Currency. He served as Acting Chief Counsel from October 2004 to August 2005. As Deputy Chief Counsel, Mr. Stipano supervises the OCC's enforcement, compliance, litigation, community and consumer law and administrative and internal law divisions. He also supervises the OCC district council staffs in the OCC's southern and western districts. Quite a busy portfolio he has.

Mr. Stipano received his J.D. from the Marshall-Wythe School of Law at the College of William and Mary in 1983. He also received a B.A. degree from Union College in 1980.

And finally, Mr. Scott Alvarez is the General Counsel for the Board of Governors of the Federal Reserve System. Mr. Alvarez joined the Board in 1981 as a Staff Attorney and became a Senior Attorney in 1985. In 1989, Mr. Alvarez was then appointed to the Board's official staff as the Assistant General Counsel and was named Associate General Counsel in 1991, and then became General Counsel in 2004.

He has had quite a distinguished career at the Fed and he has worked with Board members and senior staff to develop policies and legal positions on domestic banking issues. He has been responsible for legal analysis relating to bank acquisitions and mergers.

He earned a B.A. in economics from Princeton University in 1977 and a J.D. from Georgetown University of Law Center in 1981.

Thank you for coming back before our subcommittee. You all are familiar with the lighting system. Green means go. Yellow means hurry up. Red means stop. You will have 5 minutes to summarize your opening statements. I would just counsel you that these microphones are very directionally sensitive. They are the best of modern technology from 2 decades ago, so please use them appropriately and bring them very close to your face and mouth.

And we will now recognize Mr. Delery for 5 minutes.

STATEMENT OF THE HONORABLE STUART F. DELERY, ASSISTANT ATTORNEY GENERAL, CIVIL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. DELERY. Thank you, Mr. Chairman.

Chairman McHenry, Ranking Member Green, and members of the subcommittee, thank you for inviting me here today. And thank you for providing me and the Department the opportunity to describe our work that is designed to protect consumers from fraud perpetrated by certain merchants, third-party payment processors, and banks.

The Justice Department has made it a priority to fight consumer fraud of all kinds. Fraud against consumers comes in many forms, from telemarketing fraud to mortgage fraud, from lottery scams to predatory and deceptive online lending, and often strips our most vulnerable citizens of their savings and even their homes.

The Civil Division's Consumer Protection Branch, along with the Criminal Division and the United States Attorneys' offices across the country, has worked for decades to protect the health, safety, and economic security of the American consumer. Based on its years of experience in combating fraudulent merchants and by following the flow of money from fraudulent transactions, the Department has learned that some third-party payment processors, which are intermediaries between banks and merchants, know that their merchant clients are engaged in fraud, and yet continue to process their transactions in violation of Federal law.

Further, our experience in these cases has been that some banks, in violation of the law, either know about the fraud that they are facilitating or are consciously choosing to look the other way. As a result, in November 2012 our attorneys proposed a concentrated effort to pursue the fraud committed by the banks in paying the processors as a complement to the other consumer protection work that we are doing.

This strategy aims both to hold accountable those banks and processors that violate the law and to prevent access to the banking system by fraudulent merchants. This effort is sometimes referenced as "Operation Choke Point." One of our investigations has now been resolved and provides a useful example of our work in this area.

In April, a Federal district court in North Carolina entered a consent order and approved a settlement agreed to by the Department and Four Oaks Bank. According to our complaint, Four Oaks allowed a third-party payment processor to facilitate payments for fraudulent merchants despite active and specific notice of fraud.

For example, Four Oaks received hundreds of notices from consumers' banks, including statements by accountholders, under penalty of perjury, that the people whose accounts were being charged had not authorized the debits from their accounts.

Four Oaks had evidence that more than a dozen merchants served by the payment processor had a return rate over 30 percent—a strong sign that the bank was facilitating repeated fraudulent withdrawals. Indeed, one merchant had a return rate over 70 percent. Four Oaks also had evidence of efforts by merchants to conceal their true identities.

So according to our complaint, despite these and many other signals of fraud, Four Oaks permitted the third-party payment processor to originate approximately $2.4 billion in debit transactions against consumers' bank accounts. As the Four Oaks bank case demonstrates, the Department's policy is to base its investigations

on specific evidence of unlawful conduct. Nevertheless, in recent months we have become aware of reports suggesting that these efforts instead represent an attack on businesses engaged in lawful activity.

And I thank you for the opportunity to clear up this misconception. Our policy is to investigate specific unlawful conduct, based on evidence that consumers are being defrauded, not to target whole industries or businesses acting lawfully, and to follow the facts wherever they lead us, in accordance with the law, regardless of the type of business involved.

Now, as with virtually all of our law enforcement work that touches on regulated industries, our work in this area includes communication with relevant regulatory agencies. Such communication is designed to ensure that we understand the industry at issue and that we have all the information we need to evaluate enforcement options in light of the evidence we uncover.

That is nothing new. And for many years, banking regulators have warned banks about the heightened risk to consumers associated with third-party payment processors. In some of that guidance, the FDIC has explained that although many clients of payment processors are reputable merchants, an increasing number are not, and should be considered high risk. The FDIC has provided examples of high-risk merchants for purposes relevant to its regulatory mission.

The Department's mission, however, is to fight fraud. And we recognize that an entity that is simply doing business with a merchant considered high risk is not fraud. So in summary, our efforts to protect consumers by pursuing fraudulent bank activity are not focused on financial institutions that merely fail to live up to their regulatory obligations or that unwittingly process a transaction for a fraudulent merchant.

But when a bank knows or it is willfully ignorant to the fact that law-breaking merchants are taking money out of consumers' accounts, we will take action. So thank you, once again, and I look forward to answering the questions that you and the members of the subcommittee may have.

[The prepared statement of Mr. Delery can be found on page 45 of the appendix.]

Chairman MCHENRY. Mr. Alvarez, you are recognized for 5 minutes.

STATEMENT OF SCOTT G. ALVAREZ, GENERAL COUNSEL, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Mr. ALVAREZ. Chairman McHenry, Ranking Member Green, and members of the subcommittee, thank you for the opportunity to testify about the Federal Reserve's supervisory activities relating to banking organizations and their account relationships.

The Federal Reserve believes it is important that banking organizations provide services to consumers and businesses whose activities comply with applicable law. It is equally important that banks do not facilitate or participate in the illegal activity.

To this end, Congress, through the Bank Secrecy Act (BSA), requires banking organizations to establish and maintain programs designed to detect when services provided by the organization are

being used for illegal purposes. Under the BSA, Federal Reserve-regulated institutions, like other depository institutions, must have an effective program for knowing and performing due diligence on their customers.

Importantly, banking organizations must identify and report known or suspected violations of the BSA and other Federal laws, including reporting suspicious transactions related to money laundering activity. Criminal prosecutors at the Department of Justice and other law enforcement officials have direct access to the database that holds these suspicious activity reports and use this information to initiate investigations.

The Federal Reserve and the other Federal banking agencies have published an examination manual intended to provide practical and flexible guidance to examiners and banking organizations regarding acceptable customer due diligence and risk mitigation practices as part of an effective BSA program.

Banking organizations are expected to have a risk assessment program that takes a number of factors into account in the review of customer relationships, including the standards the organization has in place to ensure compliance with applicable law, and the relationship that the customer seeks with the banking organization.

The purpose of these policies is to ensure that banking organizations provide services to law-abiding customers. The decision to establish, limit or terminate a particular customer relationship is a decision for the banking organization. It is not the Board's policy to discourage banking organizations from offering services to any class of law-biding financial services customers.

Many of the questions that have arisen with respect to the customer due diligence expectations of the Federal banking agencies relate to the involvement of non-banks as intermediaries or providers of financial services, including money services businesses (MSBs) and third-party payment processors. Money services businesses provide financial services such as check cashing, money remittance, and similar payment services. Some MSBs include large, globally active companies, while others are small businesses such as gas stations and convenience stores offering financial products and services.

By comparison, third-party payment processors are the bank customers who provide payment processing services to merchants and other entities, such as telemarketers and online businesses. Both MSBs and TPPPs engage in transactions with individuals and companies who are not direct customers of the bank. The Federal Reserve follows an interagency examination manual and guidance issued in 2005 by the Federal Banking agencies and the Treasury's Financial Crimes Enforcement Network (FinCEN), governing account relationships with MSBs. That guidance confirms that banking organizations may provide banking services to MSBs that operate lawfully.

The Federal Reserve also follows the interagency examination manual and related guidance issued by FinCEN when evaluating the procedures banking organizations use to manage account relationships with third-party payment processors. The objective of this guidance and the Federal Reserve supervisory activities is to direct banking organizations to take appropriate steps to offer their serv-

ices to legitimate and law-abiding customers and to minimize the risk of facilitating money laundering, terrorist financing or other illicit activity.

Finally, "Operation Choke Point" is an initiative of the Department of Justice. The Department of Justice has the sole authority to indict or seek criminal fines or other sanctions and to criminally prosecute individuals or businesses for their actions.

As we have testified previously, the Federal Reserve cooperates with the other agencies in various enforcement actions, including by providing information in response to subpoenas and other requests issued by the Department of Justice and the other Federal law enforcement authorities.

Thank you for the opportunity to present the Federal Reserve's view on these important issues, and I am pleased to answer any questions you may have.

[The prepared statement of Mr. Alvarez can be found on page 38 of the appendix.]

Chairman MCHENRY. Mr. Osterman, you are recognized for 5 minutes.

STATEMENT OF RICHARD J. OSTERMAN, JR., ACTING GENERAL COUNSEL, FEDERAL DEPOSIT INSURANCE CORPORATION

Mr. OSTERMAN. Good morning, Chairman McHenry, Ranking Member Green, and members of the subcommittee. I appreciate the opportunity to testify today on behalf of the Federal Deposit Insurance Corporation (FDIC) on the FDIC's supervisory approach regarding insured institutions establishing account relationships with third-party payment processors.

I also will discuss the FDIC's interaction with the Department of Justice's consumer fraud initiative, "Operation Choke Point." As the primary Federal regulator of State-chartered financial institutions that are not members of the Federal Reserve System, the FDIC is responsible for supervising these institutions for adherence with safety-and-soundness standards, information-technology requirements, the Bank Secrecy Act, other anti-money-laundering laws, and consumer protection laws.

The USA PATRIOT Act, enacted in 2001, added new due-diligence requirements for banks under the Bank Secrecy Act, including requiring banks to establish and maintain a customer identification program. The purpose of the program is to enable banks to form a reasonable belief that they know the true identity of each customer.

In its most basic form, knowing one's customer serves to protect banks from the potential liability and risk of providing financial services to an unscrupulous customer, and also to help protect the general public against illegal activity, including terrorist financing and money laundering, since banks are a common gateway to the financial system.

The vast majority of transactions passing through financial institutions and payment processors are legitimate, and initiated by reputable merchants. However, certain kinds of business transactions or geographic locations may pose greater risk for suspicious or illegal activity.

Where transactions from a customer or merchant client of a bank's third-party, payment-processor customer are not legitimate, there is a real risk for the bank, because it can be held legally responsible for facilitating those activities and transactions. Harm to the bank can range from operating losses attributable to unanticipated consumer reimbursements, to civil or criminal actions for facilitation of violations of law.

As challenging as it can be for financial institutions to understand the risks involved in activities of a direct customer, the difficulty is magnified when the activities involve third parties. Third-party payment processors may have relationships with numerous merchant clients for which they initiate transactions.

As the financial services market has become more complex, the Federal banking agencies—the Federal Financial Institutions Examination Council (FFIEC) and the Financial Crimes Enforcement Network (FinCEN)—have issued additional guidance on several occasions alerting financial institutions to emerging risks, and suggesting mitigation techniques. Most recently, in September of last year, the FDIC issued guidance that clarifies and reminds institutions of the agency's policy on supervisory approach.

It states that financial institutions that properly manage relationships, and effectively mitigate risks, are neither prohibited nor discouraged from providing payment-processing services to customers, regardless of the customers' business models, provided they are operating in compliance with applicable State and Federal law.

The FDIC re-emphasizes policy to address any confusion that may have existed about our supervisory approach. We have reiterated this policy to our bank supervision managers and examiners to ensure that they are following this policy.

In early 2013, the FDIC became aware that DOJ was conducting an investigation into the use of banks and third-party payment processors to facilitate illegal and fraudulent activities. The FDIC has a responsibility to consider the potential risks such activities could pose for safety and soundness of our institutions.

We frequently coordinate with other agencies in supervision of our institutions. Accordingly, FDIC staff communicated and cooperated with DOJ staff involved in "Operation Choke Point" based on an interest in DOJ's investigation into potential illegal activity that may involve FDIC-supervised institutions. FDIC attorneys were performing their duties as lawyers for the agency in furtherance of the FDIC's mission.

In conclusion, our supervisory approach focuses on assessing whether financial institutions are adequately overseeing activities and transactions they process, and appropriately managing and mitigating risks. We are not focused on particular businesses.

Each bank must decide the persons and entities with which it wants to have a customer or business relationship. Financial institutions that properly manage customer relationships, and effectively mitigate risks, are neither prohibited nor discouraged from providing payment-processor services to customers, regardless of the customers' business models, provided they are operating in compliance with applicable laws.

Thank you, and I am happy to respond to the subcommittee's questions. Thank you.

[The prepared statement of Mr. Osterman can be found on page 51 of the appendix.]

Chairman MCHENRY. And finally, Mr. Stipano.

STATEMENT OF DANIEL P. STIPANO, DEPUTY CHIEF COUNSEL, OFFICE OF THE COMPTROLLER OF THE CURRENCY

Mr. STIPANO. Chairman McHenry, Ranking Member Green, and members of the subcommittee, thank you for the opportunity to appear before you today as the subcommittee reviews the Department of Justice's "Operation Choke Point" investigation.

I have spent over 20 years working on Bank Secrecy Act and anti-money-laundering issues, and have witnessed many cases where banks have been used, wittingly or unwittingly, as vehicles for fraud, money laundering, terrorist financing, and other illicit activities.

Ensuring that banks have strong systems and controls in place to deter these abuses is an important objective of the Office of the Comptroller of the Currency's (OCC's) supervision. The OCC is not part of "Operation Choke Point," so my testimony today will focus on the OCC's supervisory policies and actions.

However, it is our policy to cooperate with law enforcement investigations. And the OCC routinely receives and processes requests for information from law enforcement agencies. Some of the official requests for information we received from DOJ during 2013 were related to "Operation Choke Point."

As the subcommittee is aware, the OCC's primary mission is to charter, regulate, and supervise national banks, Federal savings associations, and the Federal branches and agencies of foreign banks. In carrying out this mission, the OCC requires banks to appropriately manage their risks, meet the needs of their communities, comply with laws and regulations, and provide fair access to financial services and fair treatment to customers.

The safety and soundness of an institution, indeed its very viability, can be threatened when a bank lacks appropriate risk management systems and controls. I have seen firsthand the serious consequences for a bank when these controls are missing.

A 2008 OCC enforcement action against Wachovia Bank illustrates this point. Wachovia failed to properly oversee activity in its third-party payment-processor accounts, and ignored significant red flags indicating consumer harm.

Telemarketing customers of the payment processors deliberately targeted vulnerable populations, such as the elderly, for the sale of products of dubious or no value. The telemarketers used high-pressure sales calls to convince these consumers to provide their personal checking-account information.

Payment processors then used consumers' account information to create checks that were deposited into the payment processors' accounts at the bank. The bank received hundreds of complaints, and hundreds of thousands of the checks created by the payment processors were returned.

Despite these red flags and clear knowledge that consumers were being harmed, the bank failed to properly address the situation. As a result of these failures, the OCC cited the bank for unsafe or unsound practices, and unfair practices in violation of the Federal

Trade Commission (FTC) Act, and required it to pay approximately $144 million in fines, restitution to consumers, and other relief.

The OCC did not, however, require the bank to cease doing business with any third-party payment processors or telemarketers. Rather, the OCC's action was focused on requiring the bank to remediate specific consumer harm, and to establish enhanced risk-management policies in order to mitigate the risk of future harm to consumers.

Currently, there is great concern that banks are terminating the accounts of entire categories of customers. And some have suggested that regulators are dictating these actions. As a general matter, the OCC does not direct banks to open, close, or maintain individual accounts, or recommend or encourage banks to engage in the wholesale termination of categories of customer accounts.

In rare cases where the bank cannot properly manage the risk presented by a customer, or a customer has engaged in suspected criminal or other illegal activity, we may order the bank, through an enforcement action, to terminate the customer's account. We expect banks to assess the risks posed by individual customers on a case-by-case basis, and to implement appropriate controls to manage their relationships.

We recognize that the controls banks put in place to manage their risks are matters of banker and supervisory judgment. If the bar is set too high, it can cause banks to terminate accounts of legitimate businesses. However, if the bar is set too low, the consequences can be dire, allowing the bank to be used to facilitate criminal and other forms of misconduct.

At the OCC, we strive to take a supervisory approach that is reasonable, balanced, and fair, and results in systems and controls that are effective in deterring the use of our Nation's financial institutions for illicit purposes.

Thank you, again, for the opportunity to appear before the subcommittee today, and I will be happy to answer your questions.

[The prepared statement of Mr. Stipano can be found on page 60 of the appendix.]

Chairman MCHENRY. I thank the panel, and I will begin with a slide on the screen, if you will all take a look at it as I give you some context. This PowerPoint slide was presented at a September 2013 conference by financial regulators in the Department of Justice for third-party payment processors.

As you can see, this list includes: "High Risk Merchants/Activities." Included on that are: "Firearm Sales, Ammunition Sales, and other lines of business."

In essence, this is a government hit list of industries telling banks to sever ties with these merchants from these industries. So, who created this list? That is what I would like to ask the panel.

Mr. Delery, did the Department of Justice create this list?

Mr. DELERY. Mr. Chairman, no. This is not a DOJ list.

Chairman MCHENRY. Okay. Mr. Osterman, did the FDIC create this list?

Mr. OSTERMAN. Chairman McHenry, the list was—actually, it first came up in the context of a Supervisory Insights Journal article that was written, I believe, back in 2011.

Chairman MCHENRY. Did the FDIC create this slide for the 2013 Third-Party Payment Processors Relationships Conference?

Mr. OSTERMAN. I think that slide would have been on the—I believe it was a slide that was used during the conference by an FDIC individual.

Chairman MCHENRY. Okay. By the FDIC, okay. So to that end, why did the FDIC pick out these particular industries for banks to consider as high risk?

Mr. OSTERMAN. It is interesting, because as I said—

Chairman MCHENRY. It is interesting, but please tell me why.

Mr. OSTERMAN. Sure. So actually, it is drawn from the industry itself. We were asked to provide examples of high-risk activities, merchant categories associated with high-risk activities, so banks and institutions could know where they needed to heighten due diligence.

And it is really drawing from situations where you are dealing with highly regulated entities where certain things may be legal in some States and not legal in others. Or where some things are prohibited, you have higher incidence of—

Chairman MCHENRY. I understand.

Mr. OSTERMAN. —chargebacks.

Chairman MCHENRY. Yes.

Mr. OSTERMAN. So it is basically—

Chairman MCHENRY. Mr. Stipano, to ask—

Mr. OSTERMAN. —the industry.

Chairman MCHENRY. Mr. Stipano, you, as well, are a prudential regulator. Do you have a similar list? Does the OCC use a similar list for targeting industries?

Mr. STIPANO. No. We do not tell banks with whom to do business. Our issue is making sure that banks have systems and controls in place to manage the risks that are posed—

Chairman MCHENRY. So that is a case-by-case basis?

Mr. STIPANO. Well, no. We would expect all banks to have systems and controls to manage their risks.

Chairman MCHENRY. No, no, what I am saying is, you will target fraudsters on a case-by-case basis, not based on a full industry, locking them out from financial services?

Mr. STIPANO. Yes, I think that is—

Chairman MCHENRY. Okay. Thank you.

And so, to continue this questioning, I would go back to Mr. Osterman. Do you see the divide here? You can see you have put out this list and it says, "Don't do business." That is what the banks have heard. "Don't do business with these full lines of industry."

Isn't that problematic?

Mr. OSTERMAN. It has certainly been misinterpreted. And that is why we put out guidance in September saying we are not saying to banks you can't do business with any entity. It is up to you to do business with whomever you want. These industries, these merchants have been identified by the payments industry as entities that have been—

Chairman MCHENRY. Okay, to that end, I will—Mr. Delery, you can flip through the binder in front of you, tab 15, just so you have context for your e-mail. Two months after this presentation, you

were told that some banks are exiting high-risk lines of business, and I am quoting from that e-mail of talking points given to you.

Does the Department of Justice use this list in "Operation Choke Point?"

Mr. DELERY. Congressman, as I indicated before, our investigations are focused on specific instances, specific evidence of unlawful conduct based on evidence that consumers are being defrauded, not participation.

Chairman MCHENRY. I hear you, but I am asking you a question about the e-mail before you that you received on talking points related to "Operation Choke Point."

It uses the same terminology here, high-risk merchants, to describe banks exiting that full industry. Is that the Department of Justice's stance?

Mr. DELERY. So—

Chairman MCHENRY. If the answer is no, it would be helpful if you just say no, that is not the Department of Justice's stance. I think that will be a satisfactory answer, if it is in fact true.

Mr. DELERY. Congressman, no, that is not the Department's stance. And we have taken steps in response to concerns that have been raised to make clear to the public and to industry that we are focused on evidence of particular fraud by financial institutions, not participation—

Chairman MCHENRY. So the fact that you are given talking points that use the exact same terminology from this PowerPoint presentation targeting these industries is merely a coincidence?

Mr. DELERY. Congressman, I would need to go back and look at the context for this. But what I can say is that our policy is to, again, focus on fraud where banks and financial institutions are knowingly facilitating fraudulent transactions or deliberately looking the other way. We are not interested in the participation of any particular industry. And participation in a lawful business has not been a factor in deciding on any of the subpoenas, for example, that I have authorized.

Chairman MCHENRY. We will now go the ranking member of the full Financial Services Committee, Ms. Waters, for 5 minutes.

Ms. WATERS. Thank you very much, Mr. Chairman. But I am not thanking you for holding this hearing. In my estimation, this is a little bit ridiculous and a waste of time.

Let me thank our witnesses here today for doing your job. This is exactly what some of us expect you to do. I want you to know that many of us are aware of activities that are fraudulent that are being perpetrated on the most vulnerable in our society. Oftentimes, you have the poorest of communities who are the victims of many of these schemes and fraudulent activity.

So I am very, very pleased about "Operation Choke Point." I want you to be as aggressive as you can possibly be.

A point of contention is how the Operation is being conducted and what methods the Justice Department is using to gather information related to fraud. Can you just once and for all repeat the legal authority that Justice uses in the Financial Institutions Reform, Recovery and Enforcement Act (FIRREA) to help protect vulnerable consumers?

Is there anything new or unique about the investigative or procedural methods being used in "Operation Choke Point?" Where does your authority come from under FIRREA? What would the effect be of amending FIRREA to restrict the Department's authority to bring these kinds of cases?

How else do you use FIRREA? What other examples or cases can you give where FIRREA has been used?

We just don't understand why anybody would think that you would target legal, lawful businesses? That would be a waste of time. It would prove nothing. So could you just please relate to some of the points that I am asking, Mr. Delery?

Mr. DELERY. Yes, thank you, Congresswoman. I would be happy to respond to some of those points.

On the question of legal authority, FIRREA is a statute that prohibits fraud affecting federally-insured financial institutions. It is a powerful tool that the Department uses in a wide variety of contexts to prevent fraud in the financial system and to maintain the integrity of the financial system.

So just yesterday, for example, the resolution that was announced with respect to Citibank, the $7 billion resolution, was based on FIRREA. It is a powerful tool that we use in a variety of contexts.

This set of investigations flows from our longstanding work targeting fraud against consumers of all kinds. There is an endless variety of scams that affect consumers, and probably all of us know a family member or neighbor or coworker who has been victimized by consumer fraud.

One thing that many scams have in common, though, is the need for access to the banking system in order to get the money out of consumers' accounts. And so, by following the money from the investigations of fraudulent merchants, including the Wachovia case that Mr. Stipano mentioned earlier, our lawyers and our investigative partners realized the roles that some payment processors and some banks were playing in knowingly facilitating fraud.

Seeing red flags of fraud, hundreds of complaints, return rates of 30, 50, 70 percent demonstrating repeated fraudulent transaction, and so as a complement to the work that we do to target lottery scams and telemarketing scams of all kinds, we have focused these cases on banks and financial institutions that are knowingly participating or deliberately turning the other way when they see red flags of fraud.

We believe that is illegal and the Department is committed to pursuing that, just as we are committed to pursuing other types of fraud.

Ms. WATERS. And I thank you for your work. I was just reading about the $7 billion settlement with Citibank.

Whether we are talking about Citibank or any of the other banks, HSBC, et cetera, et cetera, OCC—I have a bill on money laundering. And we know that it is, if I have any criticism at all, it is that yes, the fines are bigger, but it is not enough. Somebody needs to go to jail.

Somebody needs to go to jail on some of these schemes on money laundering and some of the other kinds of high-risk activities that you have listed here.

So, I don't want you to be intimidated by this hearing today. I want you to work at this. I want you to go harder at it. And Justice Department, let's put somebody in jail for the pain and the suffering that some of our consumers experience based on some of these schemes and this fraudulent activity.

I yield back the balance of my time.

Chairman MCHENRY. We will now go the vice chairman of the subcommittee, Mr. Fitzpatrick of Pennsylvania.

Mr. FITZPATRICK. I thank the chairman for calling the hearing. And I want to associate myself with some of the remarks of my colleagues who are also concerned with changing Constitutional standards, such as a presumption of innocence, which is a bedrock of our rule of law, sometimes using a Federal regulator or perhaps pressuring Federal regulators to achieve ideological objectives of the Administration. Mr. Delery, I am looking at a memo, and I think it is tab number 2 in the documents before you, dated September 9, 2013. The subject or reference line is, "Operation Choke Point Six-Months' Status Report."

In that memo, the Department of Justice stated that in the event that a legitimate business was innocently harmed by "Operation Choke Point," it should be left to the legitimate lenders themselves to prove that they are innocent. Does this mean that you are guilty until proven innocent?

Mr. DELERY. No, Congressman. That is not—

Mr. FITZPATRICK. Let me rephrase it, then. Is it common practice at the Department of Justice, generally, and in your division that you oversee, in particular, to take the approach that if the entities that we are investigating are legitimate, that it is up to them, those entities, to prove it?

Mr. DELERY. I think no, and that is not what is happening in this context either. If I could explain a little bit about how we came to identify the institutions that we are investigating, I think that would be helpful.

This really involved the use of standard law enforcement techniques. So we got information from confidential informants. We got information from complaints that banks had made or customers who had been defrauded had made.

Mr. FITZPATRICK. Mr. Delery, you are discussing entities that you are investigating.

Mr. DELERY. Yes.

Mr. FITZPATRICK. But is it possible that when you create or somebody creates a list of whole industries and then you pressure regulators to eliminate or terminate processing relationships, payment relationships with those entities, that legitimate, law-abiding businesses in this country which employ Americans can be hurt, will lose those relationships and perhaps can lose their business?

Is that possible when you use a broad brush?

Mr. DELERY. Congressman, again, I think that this is not a situation that involves the use of a broad brush.

But I do think that we take seriously the concerns that have been raised by Members of Congress, and that we have heard from industry, and that is why we have committed to taking steps to make clear to the public and to industry groups what our policy is,

that we are investigating specific unlawful conduct based on evidence of fraud against consumers and not entire industries.

So, we have written to industry groups. We have met with industry groups to make clear what we are not doing. And that is something that we will continue to do because I agree, Congressman, that it is important that people understand the scope of our law enforcement activities and why I am happy—

Mr. FITZPATRICK. Mr. Delery, you just responded a moment ago to the ranking member that this really is about following the money. That is what "Operation Choke Point" is about. So, let's follow the money here. Mr. Delery, what is the Department of Justice 3 percent fund?

Mr. DELERY. The 3 percent fund is a fund that is, as I understand it, established by statute, and that a certain 3 percent of recoveries from certain types of cases are put into the fund and can be used for other law enforcement activities.

Mr. FITZPATRICK. In other words, the Department of Justice gets a portion of the settlements obtained from initiatives like "Operation Choke Point." Is that correct?

Mr. DELERY. I would have to—I am not sure of exactly which types of cases lead to recoveries that contribute to the 3 percent fund. It is not everything that we do. But certainly a portion of our affirmative work—

Mr. FITZPATRICK. Can you respond back to this committee in writing within a reasonable period of time as to whether or not cases settled through "Operation Choke Point" contribute to the 3 percent fund?

Mr. DELERY. We can certainly get back to you on that.

Mr. FITZPATRICK. The American people need to know more about how the Department of Justice financially benefits from these settlements. So you will commit that you will provide us with full financial disclosure. Is that correct?

Mr. DELERY. Certainly, we will answer the question about the—to the extent that the Department gets—or the Treasury gets a penalty in connection with these cases, whether any part of that goes into the 3 percent fund. I just don't know—

Mr. FITZPATRICK. And you will provide that disclosure back to the genesis, to the point where "Operation Choke Point" was created, all the way back to the beginning?

Mr. DELERY. Certainly, we can; you are asking about particular amounts. We can see if we can—we can do that, certainly.

Mr. FITZPATRICK. I yield back.

Chairman MCHENRY. I recognize Mr. Cleaver for 5 minutes.

Mr. CLEAVER. Thank you, Mr. Chairman. Are any of you familiar with the Electronic Transactions Association (ETA)?

Mr. OSTERMAN. Congressman, I am actually—I recall when we were here the last time, I think it was Chairman McHenry who had indicated that the ETA had put out some guidance in this area.

Mr. CLEAVER. Yes. They put out guidance because they were concerned about rooting out fraud in the system. Is that your understanding of—

Mr. OSTERMAN. Yes, sir.

Mr. CLEAVER. Okay. So now this high-risk merchant activity list that we have seen, this is what I am assuming the American bankers used when they wrote the story about this new—or what is perceived to be this new operation that is now under way. Is this your understanding of how that story got started?

Mr. OSTERMAN. I think there has certainly been a lot of discussion about that list of examples and the concern that entities are being targeted, which is simply not true, which is why we put out a guidance which says that.

Mr. CLEAVER. But now if the ETA, the Electronic Transactions Association, did the same thing except they are inside trying to suggest to the banking world some cautions, it is essentially the same thing, right?

Mr. OSTERMAN. As we have said, that list is not a list that we made up. It is actually drawn from the industry itself. It is examples of situations where there have been high chargebacks and consumer complaints and illegal activity.

Mr. CLEAVER. So Mr. Stipano, do you have any idea how long this—how long the OCC principles regarding risk management have been in place in terms of dealing with bank payment processors?

Mr. STIPANO. Yes, sir. They go back to at least the mid-1990s.

Mr. CLEAVER. Yes. I guess I am trying to figure out why all of a sudden something that began back in the 1990s without question is now worthy of congressional hearings. I think the Lone Ranger and Rin Tin Tin are involved now. What has happened to cause this to surface? Was it that this was printed someplace, or what has happened?

Mr. OSTERMAN. I would suggest that partially what has happened is an evolution of the financial system. We have seen the growth of the Internet. We have seen telemarketing. And so, we have seen this just mushrooming of various entities that are trying to get access to the financial system. And as a result, we are seeing more fraud.

Mr. CLEAVER. Yes, but the point I am making, perhaps poorly, is that this has been going on since the—I think the early 1990s. The same things we have been talking about on this committee, they have been going on since the 1990s. There has been an acceleration because of what you just mentioned with the advent of the Internet.

So I don't understand. If anything, we ought to have a greater understanding about Treasury and Justice and other agencies trying to make sure that consumers don't get hurt any further. Is that—am I way out there? Am I wrong, anybody? No, I didn't think so.

The U.S. Consumer Coalition, a new organization, has just pledged $5 million to fight this whole process here. And I am not sure who they are. I wish we had somebody here from their organization to explain why they are spending $5 million to fight Federal agencies which are trying to protect consumers.

That is just a question that floats out there. I don't expect anybody to answer that. I yield back the balance of my time.

Chairman MCHENRY. We will now recognize Mr. Fincher for 5 minutes.

Mr. FINCHER. Thank you, Mr. Chairman. I was curious as we were getting ready for the hearing today—and I appreciate all of the witnesses being here—where the term "choke point" came from. And the first thing is I looked up the definition. It is a term used for military strategy where a geographical feature such as a valley, a bridge, or a strait through which an armed force is forced to pass is used to greatly decrease its combat power.

Mr. Delery, why did you use—where did "Choke Point" come from? Why not call it "Operation Sunshine" instead of "Operation Choke Point?"

Mr. DELERY. Congressman, the name was the name that the lawyers who—the career lawyers who proposed this set of cases gave to the operation. And I think it refers to the fact that in order to obtain money from consumers' banks accounts, fraudulent merchants need access to the payment system.

Mr. FINCHER. I have a memorandum here, dated November 5, 2012, from Joel M. Sweet to you talking about "Operation Choke Point." And I guess before I start, the point I am trying to make is that this isn't rocket science, but it seems like this was political from day one with a term like "choke point."

You may claim to be choking off the payday lenders and their business, but really you are choking off constituents and folks in my district. The payday lending industry supports 3,015 jobs in my State. As you may know, I am from Tennessee, and the payday loan industry started in Tennessee. In 2011, the Tennessee legislature passed legislation that created one of the best payday lending regulatory systems in the country. Tennessee law prevents rollovers, caps the maximum loan rate at $500, and sets a maximum term of loan at 31 days.

The Deferred Presentment Services Act codified in the Tennessee code requires that all payday lenders be licensed regardless of the manner of service delivery, including the Internet. In 2012, the Tennessee State legislature passed reforms that required all online lenders to be licensed with the statement.

Additionally, "payment instrument" was defined to mean a check, draft, warrant, money order, traveler's check or other instrument for payment of money whether or not negotiable, and also includes any authorization for electronic payment of money.

Mr. Delery, what is the State of Tennessee—what are they doing wrong, that the Justice Department felt the need to step in and protect the consumers of Tennessee, when it is clear the State has gone to great lengths to do so and is getting it right?

Mr. DELERY. Congressman, as we have said publicly on a number of occasions, we are not investigating businesses that are acting in compliance with State law. And I think that the Four Oaks case that I mentioned earlier is maybe the best example of what we are looking at. In that case, there were particular fraudulent merchants who were engaged in deceptive practices.

Mr. FINCHER. Do you have any other cases beside that one that you always refer to? Give me another example.

Mr. DELERY. I think two others would be the First Bank of Delaware case from 2012, which I think—at this point—

Mr. FINCHER. So, three? You have more than three, right?

Mr. DELERY. And Wachovia. We have other ongoing investigations, but those are the ones—

Mr. FINCHER. Do you know there have been more complaints in Tennessee—consumer complaints against the financial industry, there have been more complaints against the banks than there have been against the payday loan industry?

Mr. DELERY. I was not aware of that, Congressman.

Mr. FINCHER. I guess my question is, I am from a district where the median income is about, I guess—I have it right here, I better make sure I get it right—$45,000, something like that. And the payday loan industry fills a gap. The average loan was about $229, which banks can't make anymore because they have been regulated to the point because of Washington that they can't make these small-dollar loans and make any money off of them.

So this industry has filled a gap for people, for single moms, for people who are struggling to make it from week to week. And it seems like from day one, "Choke Point"—just think about it, folks, "Choke Point"—has been an assault not on the payday loan industry, because the trickle-down, as we all know, doesn't touch the payday lenders. It ends up hurting my folks at home, my constituents.

So, as we go forward here—my time is up—let's be very clear what the intent is. And one day, you may just be trying to regulate soft drinks as well, that we can't have too big of a soft drink. A government that is big enough to give it to you is big enough to take it away from you.

I yield back, Mr. Chairman.

Chairman MCHENRY. We will now recognize Mrs. Maloney for 5 minutes.

Mrs. MALONEY. Thank you, Mr. Chairman, and Ranking Member Green. And thank you to all of the panelists today. I particularly am glad to see Mr. Alvarez. It is rare that you appear before this committee. So I want to take the opportunity to clarify an issue that is important to the constituency that I represent.

And I refer to the Fed's interpretation of the Collins Amendment on insurance. That interpretation, which I understand was yours, referred to the Federal Government, was that it did not give the Federal Reserve the discretion to tailor capital standards for the large insurance companies that it regulates.

I would like to ask you about a bill that recently passed the Senate that addresses this portion of the so-called Collins Amendment. Do you think that the language in Senate bill 2270 solves this problem? In your opinion, do you think that it gives the Federal Reserve discretion to tailor capital standards for insurance companies?

Mr. ALVAREZ. Thank you, Congresswoman. It is good to see you again. As you stated, the Collins Amendment puts a floor on the Federal Reserve and the other banking agencies' ability to tailor capital requirements. It requires that the minimum capital requirements for all bank holding companies, including insurance companies that own banks or insurance companies that own savings—thrifts, as well as anybody designated by the FSOC as a significant—as an SIFI, all those institutions have to have capital at least at the level that would be the minimum level for a bank.

The bill that has passed the Senate does specifically allow the Federal Reserve to adjust that capital requirement for a company engaged in the business of insurance. And the Federal Reserve will follow whatever the directive is of Congress. If Congress chooses to have a floor that is the bank floor, that is what we will follow. If Congress chooses to have more flexibility for insurance companies, that will be what the Federal Reserve will do.

Mrs. MALONEY. Thank you for that clarification. And I have a series of other questions that I would like to present in writing, for you to get back to the committee on, because I have other questions for other witnesses here today.

I would like to ask Mr. Delery, as the prior speaker indicated, there seems to be a lot of confusion about the scope of "Operation Choke Point." Can you comment on this? Is "Operation Choke Point" a DOJ task force? Or is it a novel enforcement method that the Justice Department is using? How would you describe it? What is it? Is it a special project? What is "Operation Choke Point?"

Mr. DELERY. Thank you, Congresswoman, for that question.

I think the short answer is "Operation Choke Point" is a set of investigations that were designed to investigate evidence of fraud in the banking system that facilitates fraud against consumers. That is what it is. It is using established legal authorities. Fraud has been illegal for a long time. It uses ordinary law enforcement techniques to identify the institutions that need to be investigated, like complaints from banks, and complaints from consumers who have been victimized, information that comes to light in investigations of fraudulent merchants which suggests that banks and payment processors were knowingly participating.

So we have taken evidence that we received through standard law enforcement practices and have—

Mrs. MALONEY. And this has been going on since the 1990s, the prior speaker said?

Mr. DELERY. I think that was a reference to guidance about the risks and the payment system that the regulators have provided. But—

Mrs. MALONEY. Thank you.

Mr. DELERY. —this particular set of cases arose out of cases several years ago.

Mrs. MALONEY. Thank you.

And I would like to ask Dan Stipano, you said in your testimony that in the Wachovia case, the bank had ignored significant red flags indicating that consumers were harmed. Besides a high number of chargebacks rate, can you describe what some of these red flags were?

Mr. STIPANO. Yes, Congresswoman Maloney, I would be happy to do that.

I would like to start with the chargeback rate because they were excessively high in the Wachovia case. They were in excess of 50 percent. But besides that, other red flags would include customer complaints, for example, law enforcement inquiries, and also where the money is going. If there are large volumes of payments that are heading offshore, that is sometimes a red flag.

Mrs. MALONEY. Are there different red flags for different types of bank customers?

Mr. STIPANO. They can vary depending upon the nature of the business involved, yes.

Chairman MCHENRY. The gentlelady's time has expired.

Mrs. MALONEY. Thank you.

Chairman MCHENRY. We will now go to Mrs. Wagner of Missouri for 5 minutes.

Mrs. WAGNER. Thank you, Mr. Chairman.

And I thank the witnesses for being here.

Mr. Delery, a major concern with "Operation Choke Point" is that it harms legitimate businesses. Mr. Fincher just talked about the thousands of jobs that have been lost in Tennessee. I have also heard from business owners from across Missouri and Kansas, the entire region, who say they have had to cut thousands of jobs because of "Choke Point."

How would you respond to those concerns, sir?

Mr. DELERY. Thank you for the question. I appreciate the opportunity to respond directly. I think I would respond, as we have been responding when these concerns have been raised, which is to make clear that our investigations are about particular evidence of fraud by particular organizations, not industries or businesses acting lawfully. And we have attempted to communicate that to the public and to businesses in a number of ways.

But I think it is important not to lose sight of what is at stake here for consumers. Because consumers, when they are the victim of a fraud, face devastating situations when their banks—

Mrs. WAGNER. Mr. Delery, excuse me, just so that I understand things, are you saying that DOJ is dedicated to ensuring that "Operation Choke Point" does not harm legitimate businesses?

Mr. DELERY. Absolutely, certainly, in the exercise of—

Mrs. WAGNER. Mr. Delery, did you receive a memo from your consumer protection branch addressed to you entitled, "Operation Choke Point, Six-Month Status Report," dated September 9, 2013?

Mr. DELERY. I believe that I did.

Mrs. WAGNER. You did?

Mr. DELERY. Yes.

Mrs. WAGNER. The report, which I have here, says, and I quote: "Although we recognize the possibility that banks may have decided to stop doing business with legitimate lenders, we do not believe that such decisions should alter our investigative plan." Is this DOJ policy, sir?

Mr. DELERY. As I indicated before, our policy is to make clear that we are not targeting lawful businesses, and that is what we have done so that—

Mrs. WAGNER. Wait a second here. But then, in your testimony here today, you said, sir, that DOJ is dedicated to ensuring that its efforts to combat fraud do not discourage or inhibit the lawful conduct of honest merchants. Yet, at the peak of "Operation Choke Point," in a memo sent to you, your lawyers recognize that legitimate businesses were in fact being harmed, but decided that the ends justified the means.

Are you saying, sir, that DOJ's policy has changed?

Mr. DELERY. No, Congresswoman. I think if you look at the overall context of that document, it makes it clear that the goal of—

Mrs. WAGNER. So DOJ policy has not changed? You are still targeting legitimate businesses?

Mr. DELERY. No, Congresswoman. Our policy from the beginning of the framing of these cases and to today, which we have restated publicly, is that we are pursuing evidence of—

Mrs. WAGNER. But your own lawyers have said something completely opposite to that in terms of collateral damages and going after legitimate businesses, in a sense. And I guess you have to break a few eggs in order to make an omelet.

What is your response to that, sir? There seems to be great disparity here.

Mr. DELERY. I think that if you look at the materials that have been provided, you will see that the policy and the framing of the cases was clear from the beginning. If you look at even that one as a whole, that document makes clear that the cases were about fighting fraud.

Mrs. WAGNER. Mr. Delery, clearly the DOJ's public statements to Congress do not match with its internal communications. Now, what will you do to restore the integrity to your office and ensure that no more legitimate jobs or businesses become collateral damage, so to speak, of "Operation Choke Point?"

Mr. DELERY. I think what I will do is what I have done since these concerns have been raised, which is to re-articulate the policy to the public and to the industry and internally to make clear that our investigations are focused on evidence of specific unlawful conduct that we are investigating based on evidence that consumers are being defrauded, not entire industries.

Mrs. WAGNER. Sir, are the thousands of jobs lost across the country from Missouri to Tennessee just collateral damage to the Department of Justice?

Mr. DELERY. I don't view any consequences as collateral damage. I think obviously, we take seriously the need to make clear what we are and are not doing.

Mrs. WAGNER. You haven't made it clear, sir, because your internal communications are completely different than your testimony here today. So I am asking you: Has DOJ policy changed regarding this?

Mr. DELERY. DOJ policy from the beginning—my policy, which I have articulated publicly and internally, is that these cases are about fighting evidence of fraud, not conduct of lawful businesses. And I will continue to maintain that policy and I expect that the managers and supervisors of these cases will make sure that it is implemented.

Mrs. WAGNER. Mr. Chairman, I believe my time has expired.

Chairman MCHENRY. Mrs. Beatty is recognized for 5 minutes.

Mrs. BEATTY. Thank you, Mr. Chairman, and Mr. Ranking Member.

We have heard a lot of questions posed in pretty much the same vein. Certainly, as we have been listening today and we know that "Operation Choke Point," carried out by the DOJ's Civil Division, Consumer Protections Branch, is a series of investigations and enforcement acts which are designed, most importantly, to protect American consumers from mass market fraud.

Given that, and I will start with you, Mr. Delery, and the questions that you have been attempting to answer, let me try to put it in a different vein. What, if any, evidence is there that "Operation Choke Point" may be having a deterrent effect on consumer fraud in the United States?

Mr. DELERY. Certainly, I think that is the hope that we have for our law enforcement work in this area and otherwise. We, when investigating evidence of fraud, as reflected, for example, in the Four Oaks case, when we announce a resolution of a case like that and detail the allegations and the evidence that we have related to fraud facilitated by a financial institution, our expectation is that will have a deterrent effect.

We hope that the Citibank resolution that was announced yesterday has a deterrent effect on fraud against investors. We hope that our cases involving tainted food and medicine have a deterrent effect so that other sellers don't make people sick. And in this context, we hope that there is a deterrent effect for consumer fraud. As these cases continue, we will be looking for that.

Mrs. BEATTY. Let me follow up with—because we have heard a lot about the third-party payment processors in that process. Does the DOJ bring claims against third-party payment processors or financial institutions that—let's say, unwillingly or accidentally facilitate fraudulent or unlawful activities? And if not, kind of outline or describe for us how you can be sure of that?

Mr. DELERY. Okay. Thank you, Congresswoman. I appreciate the opportunity to address that because I do think it is an important issue. Our cases are focused on knowing participation in fraudulent activity by a merchant.

So the bank or the payment processor has information, like exorbitant chargeback rates that were discussed earlier, or sworn complaints from hundreds of customers or evidence, as was the case in the Four Oaks case, evidence that the merchants were hiding their identities. We are not disclosing their true identities. Or again, in Four Oaks complaints from a State attorney general about the conduct.

So we are dealing with knowing information, not a technical violation of regulatory guidance or the unwitting processing of a particular transaction. Our subpoenas and our investigations are targeted at that kind of evidence we move forward with investigations and with actions where we can establish that was the case.

Mrs. BEATTY. And lastly, we have been hearing a lot of questions by some of my colleagues that, from where I am sitting, sounds like that you are willingly going after people who are lawfully doing what they are supposed to do. So I am sitting here, trying to figure out what would you gain by having the DOJ go after people who are lawfully operating to put them out of business? So with that in the back of my mind, are there any statements you would like to make to respond to those allegations that the DOJ's investigatory practices are designed to put good companies out of business?

Mr. DELERY. I think the best way for me to respond is to say that is not what we are doing. And the best indicator of that, I think, are the cases that we have actually brought. So the Wachovia case that has been discussed in great detail, extensive evidence of actual fraud by the financial institution, and that is true for the Four

Oaks Bank case that I have discussed, and another case called First Bank of Delaware from 2012.

So I think if you look at the track record of the cases that we have brought, they demonstrate that we are investigating fraud against consumers, which is the goal of this work. The goal of this work is to make sure that the hard-earned earning money in the bank accounts of consumers is not drained by fraudulent merchants with the cooperation of a financial institution. That is what these cases are about.

Mrs. BEATTY. Thank you very much. Thank you, Mr. Chairman.

Chairman MCHENRY. We will now go to the gentleman from Wisconsin, Mr. Duffy.

Mr. DUFFY. Mr. Delery, would you just walk me through the process and how you decide when to issue subpoenas for fraudulent activity? And if you could do it quickly, that would be wonderful.

Mr. DELERY. I'm sorry, how we decide—

Mr. DUFFY. Yes.

Mr. DELERY. On the—certainly, I think it is based on standard law enforcement approaches. So looking at information that we have obtained in one investigation that suggests that another party is involved in law enforcement activity.

Mr. DUFFY. You investigate, you get complaints, and you make a determination that there is potentially fraudulent activity, right?

Mr. DELERY. And then continue to seek more information if that makes sense.

Mr. DUFFY. And then when you have enough information, you send a subpoena to the banks, correct?

Mr. DELERY. Yes. When we have reason to believe that there is fraudulent activity, we—

Mr. DUFFY. So when you have reason to believe, you send a subpoena out?

Mr. DELERY. Right.

Mr. DUFFY. And is it pretty fair to say, Mr. Osterman, that when these banks receive a subpoena from DOJ, they cease to do business with the third-party payers or with the payday lenders? Is that fair to say?

Mr. OSTERMAN. I don't know if that is fair to say. I can't speak for the banks, but the subpoena is asking you for documents. If the bank is operating lawfully and the third-party payment processor is acting lawfully there, you have nothing to be concerned about.

Mr. DUFFY. Okay. Great. So—

Mr. OSTERMAN. The reason why they wouldn't—

Mr. DUFFY. So, subpoenas are brought. You continue in your investigation. You have referenced, what, three cases in which you have brought a suit against banks, right? Four Oaks being one of them?

Mr. DELERY. Four Oaks, yes, is one of them.

Mr. DUFFY. So I am interested not in—because you keep talking about fraud in the banking system, fraudulent merchants. Are you bringing cases at the DOJ against the fraudsters? Are you bringing cases against the third-party payer, as you are bringing cases against the payday lenders?

Mr. DELERY. I think—

Mr. DUFFY. No, no. Are you bringing cases? Answer my question. Are you bringing cases against the third-party payers and the payday lenders?

Mr. DELERY. We are investigating—

Mr. DUFFY. No. So you haven't brought cases against them. That is my point.

Mr. DELERY. I have—

Mr. DUFFY. So who does—you have come in here and you have said, "Listen, we have fraudsters. They have committed fraud." Who has determined fraud? You are an attorney at the DOJ. Has there been due process? Has there been a hearing? Has there been an adjudication of fraud? No. You have come in here and said, "We have fraudsters across the country from whom we are protecting America."

There is no judicial determination of fraud. It is that we have a bureaucrat in the DOJ who says, "I think it is fraud. And so, I am going to shut down a legitimate business." Am I wrong?

Mr. DELERY. Yes, Congressman. I disagree with that summary of what we are doing and I think—

Mr. DUFFY. Then the question is, how many dispositions have you had from a court that these third-party payers or a payday lender has committed fraud, how many?

Mr. DELERY. So a number—

Mr. DUFFY. How many?

Mr. DELERY. So a number—I believe that they are—

Mr. DUFFY. The answer is zero, isn't it?

Mr. DELERY. I think, no. In connection with the Wachovia case, the third-party processor was also reviewed—

Mr. DUFFY. You don't even know. You prepared how long for this hearing and you can't tell me how many have been adjudicated fraudulent. And you have come in and you have told us, with a straight face, and a straight eye, that there is fraud and that you are protecting the American people. I am going to put up the list of high-risk merchants, so you can go after payday lenders, which—listen, there is no love for payday lenders, but the system that you are using is of concern.

You can go after payday lenders. You might say, "Well, listen, high-risk merchants—they include firearms dealers, they include ammo manufacturers, right? You can go after all of them to protect banks. And so can Mr. Osterman at the FDIC.

I think I was listening, and we heard that highly regulated industries that do business across State lines or have different regulations in different States. Another one that could be on this list if the Administration changes—could Planned Parenthood and could the abortion issue be on that list? I am not saying it should be, but who is to say that they couldn't get into a bureaucratic scheme to shut down legitimate businesses?

I look at Colorado. You have the DOJ bending over backwards to make rules work so drug dealers selling marijuana can actually bank. But here on the list, you have tobacco sales as high-risk merchants.

Our concern is, we have a Federal Government that is out of control. And we have bureaucrats who think they can get a swift idea and impose the heavy hand of government on legitimate businesses

that have had no adjudication of fraud. But you come in here and you say, "Fraudulent, fraudulent, fraudulent," and you haven't proved it at all.

I yield back.

Chairman MCHENRY. All right.

The gentleman from Washington, Mr. Heck, is recognized for 5 minutes.

Mr. HECK. Thank you, Mr. Chairman. I want to also thank the gentleman from Wisconsin for the seamless segue to my line of inquiry. Mr. Osterman, I had intended to ask you about "Operation Choke Point." But then last night, with my 12-hour-old edition of USA Today, I opened it up, and there on page one was an article that was entitled, "Pots of Marijuana Cash Cause Security Concerns." Among other things indicated in this article is a security expert saying about marijuana businesses in States where it has been legalized, either for medical use or for adult recreational use, "Some people walk in with shoeboxes full of cash. Some people walk in with locked briefcases. We have had people bring it in buckets. The vast, vast cash flows are a clear come-on for criminals."

And, finally, you are effectively creating a magnet for crime. I have been very concerned about this public safety issue for some time. That is why I was pleased last August when the Department of Justice did, in fact, in the now-famous Cole Memorandum, set forth its conditions for standing down a prosecutorial action—remind you that the two top criteria are preventing marijuana from getting into the hands of children, and preventing cash from getting into the hands of gangs. And that was followed in February of this year—a wonderful Valentine's Day—by guidance from the Financial Crimes Enforcement Network, in which they indicated the basis on which they would not seek follow-up action.

Both of these effectively create, I guess, kind of a safe harbor, if the terms and conditions are followed. And the spirit of those terms and conditions, I think—although there are many—with the Department of Justice, it is those eight terms and conditions. And with FinCEN, it gets into the suspicious activity reports and what recording requirements are required. But the essence of them, really, is public safety. The essence of them—and I am going to repeat myself, because I think it is so very important—is to keep marijuana out of the hands of children, and keep cash out of the hands of the gangs and cartels.

Mr. Osterman, you stop short in your follow-up and implementation of this. And I guess my question really is, what, if anything, can you say today to give confidence to banks and credit unions that they can provide banking services to legally constituted legitimate marijuana businesses, without the threat that your agency will penalize them, threaten their deposit insurance, or whatever, or force them to close their accounts? Keeping in mind that this is first and foremost a public safety issue.

Mr. OSTERMAN. Congressman, the Cole Memorandum, which you referenced, as well as the FinCEN guidance, I think is very helpful. And we have actually told our examiners, when they are examining institutions, to ensure that those institutions are in compliance with those guidelines. And we have actually provided a letter to

Washington State banking authorities to that effect. And I believe we may be in the process of doing that with Colorado, as well.

Mr. HECK. It is the very letter that I am referring to, Mr. Osterman, that does not go as far as the Department of Justice, nor FinCEN's guidance in terms of basically saying, if you completely respect these terms and conditions, according to DOJ and according to FinCEN—and again, for the third or the fourth time—the essence of which is public safety—keeping marijuana out of the hands of children and cash out of the hands of gangs and criminals—then you will not pursue regulatory action. Your letter stops short of that.

What can you say today, or what follow-up correspondence might you be willing to provide that is consistent with the Department of Justice's language and form of safe harbor, as well as FinCEN's?

Mr. OSTERMAN. Again, FinCEN—these are criminal activities. FinCEN sets the standard. And they have spoken. And I think we have gone as far as I am aware that we can go. If there were any kind of guidance that would be issued, it would have to be an interagency type activity through FFIEC. And, I don't understand why that doesn't provide—

Mr. HECK. So, are you saying that if they follow FinCEN and DOJ, you will not make a regulatory sanction?

Mr. OSTERMAN. We are telling our examiners to ensure that they are doing that. If they are, we are not going to—

Mr. HECK. I would appreciate it if you could have them communicate that more clearly.

Thank you, Mr. Chairman, for your indulgence.

Chairman MCHENRY. The gentleman's time has expired. And while it is bipartisanship, it is two sides of the same leaf, perhaps.

We will now go to Mr. Barr, from Kentucky for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman.

Gentlemen, I don't know of anyone who would find fault with financial regulators who, in good faith, are attempting to stop consumer fraud. I think what the American people are troubled by—and what Members of Congress are concerned about here today—is the prospect of powerful Federal agencies working with the Department of Justice to pressure banks to terminate relationships with legitimate businesses. Now, you can understand that. You can understand why there would be concerns, in particular for lawful and legitimate businesses that may be politically unpopular with this Administration's policies.

Let me give you an example of where a Kentucky resident raised this concern with me. And in Kentucky, we have particular sensitivity with the Administration's, what we consider a very political attack, on a very legitimate business, the coal industry.

We have lost 7,000 coal-mining jobs in Eastern Kentucky over the last several years because of this Administration's regulatory assault against this very legitimate business that is employing thousands of people in our communities. We have these communities littered with unemployed coal miners, and their families are suffering as a result of Administration policy.

We got an e-mail from a Kentucky resident in our congressional office, and this is what it said: "Our family company has been in the business of leasing our land to coal producers for decades.

Today, I returned a call from Client Services at our bank in Lexington, Kentucky.

"They asked if we lease land to coal producers that operate surface mines. They said they are receiving pressure from bank regulators, and will no longer do business with us if we have surface mines on our property.

"After some thought, I called back again, and asked if we would be receiving a letter from the bank stating the situation in writing. I was told that yes, we would receive a letter, but it would not talk about pressure from regulators.

"Further, she said it would state to the effect that it is in the best interest of the bank not to do business with our company due to the perception of and its effect on their business."

So verbally, the bank is telling the customer, "The regulators are pressuring us to not do business with your family any longer."

But in writing, they won't do that. So my question to all of you is, as regulators and as the Department of Justice, are you aware of any guidance, directives or efforts by your agencies to stop financial institutions from transacting business with coal operators or land holding companies that lease their land to coal producers?

And I will just have you all go down the line.

Mr. DELERY. No, Congressman.

Mr. ALVAREZ. No, Congressman.

Mr. OSTERMAN. No, Congressman.

Mr. STIPANO. No, sir.

Mr. BARR. Have bank regulators at any time in the last 2 years ever had a policy of pressuring banks to reevaluate their relationship with coal operators, coal-production companies, or a surface-mining operation, that you are aware of? Have you ever been in meetings where the topic of coal production has ever come up in the context of "Operation Choke Point?"

[Witnesses shake heads, "no."]

Okay. I am glad to hear that, because I want to get a commitment from each of you that you will assure me that your agency will not, does not, and will not in the future discourage, either explicitly or implicitly, any financial institution from doing business with coal-mining activities, whether surface or deep mine? Can you give me that commitment?

Mr. DELERY. Yes, Congressman. As I have explained our policy, it would have nothing to do with the situation that you are describing.

Mr. ALVAREZ. Congressman, I agree with the notion that you are trying to come across, bring across about dealing with an industry. I can't say that there isn't going to be some coal individual supplier that may not have financial difficulties where a bank may choose not to be involved with them because of that.

So putting aside the kind of credit quality, and other kinds of normal banking criteria, I agree with you.

Mr. OSTERMAN. I think Mr. Alvarez has stated it appropriately. We do have underwriting standards that the banks would be looking at, and safety-and-soundness standards. But given the context in which you are raising this, I can agree with—

Mr. BARR. And I only have 10 seconds left. I just want to make sure that when you are looking at fraudulent activity, you are not

defining a risky business. So, you are not targeting risky businesses in a way that is in any way advancing the EPA's agenda?

Mr. DELERY. No, Congressman. We are looking at fraud against consumers.

Mr. BARR. Thank you for your commitment that you will not further the war on coal. Thank you. I yield back.

Chairman MCHENRY. And the record will note soft sighs of "no" are still noted as "no" in the record. We have talked enough about the microphones, but they are quite lackluster.

We will now go to Mr. Kildee, of Michigan.

Mr. KILDEE. Thank you, Mr. Chairman. And I want to thank the witnesses for not only your testimony, but for the work that you have been doing in protecting the American consumer, which after all, is sort of the point of the activities that we are designed to get at here.

I want to make a couple of quick observations, and then ask for some commentary from the panel. Number one, I think we all understand political theater. And I have a sense that I am participating unwittingly in a bit of political theater today. It is certainly not my intention, but that seems to be what is happening here.

From questions about how the name was selected for this operation, I think somebody suggested, "Operation Sunshine." Next time you do this, maybe you should do, "Operation Powder Puff," and it might not be so offensive to some. Frankly, it is a ridiculous question, and I regret that you had to answer it.

To a comment that, why are we worried about this, the average payday loan in one State is only $227. Well, this is something that we have been looking at. I think about the case of the soldier who borrowed $1,600, and after 2½ years, had repaid $17,000 to the lender.

So that $1,600 might not seem like a lot to some people in this room. But $17,000 for a $1,600 loan raises a bit of suspicion, and I think would indicate that there are some commercial practices, some entities, some enterprises, some areas of business, that might be legitimately subject to scrutiny. And that is exactly what this is intended to do.

So let me ask just quickly two things. One, there was much made of this slide, which indicates examples of commercial enterprises for which this sort of scrutiny might ultimately be applied.

I would like whomever would like to, to offer a commentary on how a list such as this might be derived. Presumably, it is based on consumer complaints, return rates, real data, that would lead one to conclude that if you are going to be looking for fraudulent activity, it makes sense to look at it where there is a greater likelihood that it is taking place. If you could just comment on that?

Mr. OSTERMAN. I would be happy to respond. This group of examples actually was taken from actual experience that the industry has actually had over the course of years.

The problem that we have had is that it has been turned into something that it is not, which is you can't do business with these people. And that is why last year we issued guidance making it very clear that banks can do business with whoever they want to. They just need to have appropriate risk mitigation factors in place.

Mr. KILDEE. I guess the other question that I would have is what your response is to this notion that there is an agenda behind that, which is intending to sort of steer commercial or lending activity, or banking activity, away from one industry to another.

And the implication which is being suggested is that because certain financial institutions may, of their own volition, decide that there is an area of enterprise that they have found to be problematic, that they make by themselves, a market-based decision that they are going to move from that: first, is that something that you are seeing in large numbers; and second, is that an illogical conclusion for a financial institution to make to say, "I think we are going to sort of get out of financing activities in this category of, let's say, payday loans, or gambling?"

Does it make sense to you that might be a legitimate business decision that a for-profit enterprise might make, just as a matter of course?

Mr. OSTERMAN. I think that these are business decisions that businesses make in terms of their risk tolerance and their underwriting standards. Again, it is a decision for those businesses to make. It is not for the government to make, and it is not one the government is making.

All we are saying is some types of activities are higher risk, and you need to have appropriate risk mitigation measures in place.

Mr. KILDEE. I would just encourage all of you to continue to do the work you are doing to protect consumers. And I know you won't, but I encourage you to not take sort of the threat of political speech accusing you of trying to shut down legitimate businesses, which I know you are not, as an excuse to not protect consumers who clearly need the protection of their government.

So I want you to continue your work in that effort, and I appreciate it. Thank you.

Mr. FITZPATRICK [presiding]. The Chair recognizes Mr. Luetkemeyer for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman. Gentlemen, I appreciate the job that you do with regard to trying to root out fraud. Unfortunately, what we have done today, "Operation Choke Point," is going well beyond fraud. It has gone beyond that.

As we have heard this morning multiple times, it is now going to an industry-based approach to try and get rid of everything and everybody in that entire industry, versus only the bad actors in industry, which is wrong. You know it is wrong, I know it is wrong.

We discussed this, Mr. Delery and Mr. Osterman. And we discussed this individually. I thank you for the letters that we received as a result of you trying to clarify your position that as long as a business is doing a legal business, the legal entities are okay.

Gentlemen, we have a problem. It is continuing. It has not gone away, has it? I can tell you, I can sit here this morning and give you case after case of what I have been talking about. I have here in the paper a document by the newspapers.

Friday, May the 30th, there was a gun manufacturer in Hyannis Port, Massachusetts. Here is one from the 19th of May which talks about a firearms training supply company in Florida. Here is an armory in Nevada.

So, gentlemen, it is not a rogue agent doing this. It is not a rogue examiner. It is still going on. It is still going on now. What are you going to do to stop it? Mr. Osterman?

Mr. OSTERMAN. Congressman Luetkemeyer, what we have done is we have tried to be very clear in putting out our guidance to say very publicly and clearly that as long as banks have appropriate risk mitigation measures in place, we are not going to prohibit or discourage them from doing business with anyone with whom they want to do business.

And we have said that. We have actually had meetings with our examiners. Our division directors have met with our examiners, and sent that message to them. And we have even sent that notice to the banks themselves and said, "If you are aware of this happening, let us know."

Mr. LUETKEMEYER. Mr. Osterman, with all due respect, you know and I know, as a former examiner, and you know it, that the banks are scared to death when an examiner comes in there and threatens them. There is that problem.

And I have talked to the bankers about this. And I said, okay, if they are telling you to do away with an entire book of business, which is going on, I said, have you asked them to put it in writing? And they said, yes. What would they say? And they say the examiner refused to do that.

So the examiner is not giving them the documentation to give you the track to go back to that individual. As we see here, it is not going on in one State. It is going on across the country.

This has to be something that has to be concerning to you if you are worried about this. If you are not—I discussed with Mr. Delery and you guys both about putting in place a safe harbor. Both of you have—both of your agencies have denied wanting to work with us on that.

The other day, we had the CFPB in here, and we tried to ask them also if they would put together a safe harbor for the banks to be able to do business with legitimate customers that they have been doing business with for the last 25 years.

I had a banker tell me he had to get rid of customers who had been with him for 25 years, for no reason other than the examiner said, "Hey, you can't do business with these guys anymore because they are in an industry that is under heightened scrutiny."

So as a result of that, I offered a bill a couple of weeks ago that is going to put in place a safe harbor. Would you guys be willing to support that? Mr. Delery?

Mr. DELERY. Congressman, we certainly have seen the bill that you offered. We are reviewing it and we will obviously continue to do that and work with you and your office on it.

I think that what is important, from our perspective, is that we maintain the tools that are necessary to fight fraud against consumers. We have attempted in—

Mr. LUETKEMEYER. To that effect, we want to work with you, but you haven't been able to work with us. You haven't been honest with me. Mr. Osterman, are you willing to work with us on a safe harbor? How come we haven't gotten together yet?

Mr. OSTERMAN. We would be willing to work with you.

Mr. LUETKEMEYER. Do you like my bill?

Mr. OSTERMAN. We have concerns. Frankly, there are difficulties in trying to create a safe harbor in terms of avoiding unintended consequences.

Mr. LUETKEMEYER. So you are telling me by going around the corners here, which you are doing this morning, it gives me great pause, the fact that we are still doing this. And now you won't go along with the safe harbor. You are saying, we can't do this, can't do that.

It tells me you are not willing to give up "Choke Point." You are willing to continue to go out here and do a broad-brush approach to get rid of the entire industry, and that is wrong.

Mr. Delery, one more quick question. The gentleman who was in charge of putting "Choke Point" together, Mr. Joel Sweet, is that correct?

Mr. DELERY. He was the author of the original proposal, yes.

Mr. LUETKEMEYER. Why was he reassigned?

Mr. DELERY. He—now I—obviously, I need to be careful about talking about individuals in this setting, but it has been reflected in the documents that he was in Washington on detail from his home U.S. Attorney's Office. He is a career assistant U.S. attorney. He was here on a temporary detail that was 6 months. It was extended to a year, and when that ended, he went back to his home office, as was always the expectation he would do.

Mr. LUETKEMEYER. It is interesting that it happened just a few days after we got the letter.

Thank you very much. I yield back.

Mr. FITZPATRICK. I recognize the ranking member, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Mr. Chairman.

Mr. Chairman, in court we had an objection known as "assuming facts that are not in evidence." Today, we have had a lot of anecdotal commentary given to witnesses, which would cause one to assume facts that have not been placed in evidence.

We have not had empirical evidence of the allegations that have been made, the anecdotal evidence, if you will. So let's for just a moment examine some facts. Let's go to the North Carolina case and let's talk for a moment about the number of complaints that were received against this bank.

And I will start with our representative from the Justice Department, Mr. Delery.

Mr. DELERY. As reflected in our complaint that was filed in the case when the—then that led to the consent decree that the court approved, the bank had received hundreds of complaints from banks of customers who had been victimized, that included sworn statements.

Mr. GREEN. Let me intercede for just a moment. You said from banks of customers. So you have banks complaining about the activity of another bank.

Mr. DELERY. Yes, exactly, Congressman.

Mr. GREEN. And let's go on. From this material, this number of complaints, did the bank take some affirmative action without the Justice Department's intervention?

Mr. DELERY. Again, as alleged in the complaint, the bank was aware of these complaints, as well as complaints from NACHA, the

Electronic Transactions Association, and the Attorney General of Arkansas, and yet continued to facilitate the transactions of the payment processor that was handling the transactions that were—

Mr. GREEN. Let's put a face on this. These transactions were actually consumer purchases. Is that a fair statement? Or, there were consumers associated with each of these transactions? Is that a fair statement? Because these were payday loans.

Mr. DELERY. Many of them were related to payday lending, not all, but many. And they were transactions involving consumers. So the main complaint, again, as reflected in our allegations, was that the consumers had been misled into the terms and the number of debits that they understood would be coming out of their accounts.

Mr. GREEN. And is it true, sir, that the bank received about $850,000 in fees associated with these transactions?

Mr. DELERY. Yes. Again, that is the number that we have in our complaint.

Mr. GREEN. And is it true that there was a settlement for about $1.2 million, meaning that the bank agreed to pay some $1.2 million to settle this case?

Mr. DELERY. Yes, and also agreed, as reflected in the consent order, to a series of compliance measures that we insisted on to ensure that fraud couldn't occur—couldn't continue with respect to—

Mr. GREEN. Was this a product of "Operation Choke Point?"

Mr. DELERY. Yes, this was one of the cases, the investigations that arose out of that series of work.

Mr. GREEN. If not for "Operation Choke Point," would we have the $1.2 million settlement, would this bank have been put in a position such that it had to make a change such that this kind of behavior, this activity, is no longer continuing?

Mr. DELERY. Again, Congressman, I think that result is the direct result of our work in these investigations. And this case is the best example of the kind of work that we are doing. It is about real fraud, not just doing business with a lawful industry.

Mr. GREEN. Thank you.

Let me quickly go to the—I am going to call it the list of merchants. It is titled, "High-Risk Merchants Activities." Now it has been indicated to us that this list was compiled with the assistance of industry. Is that correct?

Mr. OSTERMAN. It is actually taken from industry—experienced industry examples. And in fact, it is very—

Mr. GREEN. But this is about more than industry. This is about the people who are doing business with these industries. Is that correct?

Mr. OSTERMAN. Yes.

Mr. GREEN. Is it about consumers who were being defrauded as a result of doing business with these industries? Is that correct?

Mr. OSTERMAN. Again, as we have said in our guidance, the fact that certain industries are high-risk doesn't mean—

Mr. GREEN. Doesn't mean that they are—that all of the businesses within an industry, but the complaints that are generated are usually based on some consumers saying, "You took too much money from my credit card," or "You added too much to my credit card." "You used my bank routing number and you collected money from my bank without my consent and permission."

Is that a fair statement?

Mr. OSTERMAN. Yes.

Mr. GREEN. So we are trying to, with this, the intent of this was to protect consumers. Is that a fair statement?

Mr. OSTERMAN. It is. But again, I just would caution, that list does not—

Mr. GREEN. Not yours—

Mr. OSTERMAN. It is a list that came from a supervisory insights journal that FDIC published a long time ago. But the point of it was not to say you can't do business with these entities. A lot of those entities are legitimate.

Mr. GREEN. I agree with you, but the purpose of it was to protect consumers, ultimately.

Mr. OSTERMAN. Yes.

Mr. GREEN. That was my question.

All right, Mr. Chairman, if I may, I would like to, for Mr. Heck, ask unanimous consent to make the article entitled, "Pots of Marijuana Cash Cause Security Concerns" a part of the record.

Mr. FITZPATRICK. Without objection, it is so ordered.

Mr. GREEN. And with that, I will yield back the balance of time that I do not have.

Mr. FITZPATRICK. I thank the ranking member.

With that, I would like to thank our witnesses again for their testimony today.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

And without objection, this hearing is adjourned.

[Whereupon, at 11:58 a.m., the hearing was adjourned.]

A P P E N D I X

July 15, 2014

For release on delivery
10:00 a.m. EDT
July 15, 2014

Statement by

Scott G. Alvarez

General Counsel

Board of Governors of the Federal Reserve System

before the

Subcommittee on Oversight and Investigations

of the

Committee on Financial Services

U.S. House of Representatives

Washington, D.C.

July 15, 2014

Chairman McHenry, Ranking Member Green, and other members of the subcommittee, thank you for the opportunity to testify about the Federal Reserve's supervisory activities pertaining to banking organizations and their account relationships with law-abiding businesses. In my testimony, I will describe the legal framework governing the establishment and maintenance of customer accounts and the regulatory expectations the Federal Reserve has established for the banking organizations we supervise. I will also highlight related aspects of our examination and enforcement process in this area.

Let me begin by saying that the Federal Reserve believes it is important that banking organizations provide services to consumers and businesses whose activities comply with applicable laws. It is equally important that the banks we supervise do not facilitate or participate in illegal activity. Indeed, during the past several years the Federal Reserve has provided information to the banking organizations we supervise to clarify the requirements for providing account services to law-abiding businesses.

Legal Framework and the Federal Reserve's Regulatory Expectations

Congress, through the Bank Secrecy Act (BSA), requires banking organizations to establish and maintain anti-money-laundering (AML) programs designed to detect when services provided by the organization are being used for illegal purposes. By law, each Federal Reserve-regulated institution, like other depository institutions, must have a BSA program that contains four critical elements, including a system of internal controls to ensure ongoing compliance with the BSA, independent testing of the bank's compliance with the BSA, training of appropriate bank personnel, and the designation of an individual responsible for coordinating and monitoring day-to-day compliance with the BSA.[1] Under the general rubric of "know your customer" laws

[1] See 31 U.S.C. § 5318(h) and Board of Governors Regulation H (12 C.F.R. § 208.63) (BSA program requirements for state member banks).

and regulations, each banking organization is also required to maintain a customer identification program as part of the BSA compliance program and perform due diligence on its customers.[2] In addition, a banking organization must identify and report known or suspected criminal violations of the BSA or certain other federal laws and suspicious transactions related to money-laundering activity.[3] Criminal prosecutors at the Department of Justice and other law enforcement officials have direct access to the database that holds these Suspicious Activity Reports and rely on this information to initiate criminal investigations.

The Federal Reserve and the other federal banking agencies have published an examination manual intended to provide practical and flexible guidance to examiners and banking organizations regarding acceptable customer due-diligence and risk-mitigation practices as part of an effective BSA program.[4] The Federal Reserve expects a banking organization to maintain adequate policies and procedures to address risks associated with customer relationships. The scope of these policies and procedures will depend on the banking organization's ongoing assessment of the risks posed by the particular customer relationship. A banking organization takes many factors into account when conducting a customer risk assessment including, in particular, the standards the customer has in place to ensure compliance with applicable laws and regulations, and the relationship the customer seeks with the banking organization. It is essential that banking organizations make a judgment as to customers with respect to the level of risk they pose.

---

[2] See 31 C.F.R. § 103.121 and Board of Governors Regulations H and K at 12 C.F.R. §§ 208.63(b)(2), 211.5(m)(2), and 211.24(j)(2) (customer identification requirements).
[3] See 12 C.F.R. § 208.62 and Regulations K and Y at 12 C.F.R. §§ 211.5(k), 211.24(f), and 225.4(f) (suspicious activity reporting requirements).
[4] See Federal Financial Institutions Examination Council (2010), "Bank Secrecy Act/Anti-Money Laundering Examination Manual" (April 29).

The purpose of these policies is to ensure banking organizations provide services to law-abiding customers. The decision to establish, limit, or terminate a particular customer relationship is a decision for the banking organization. This decision may be based on various factors, including a banking organization's assessment of the risks associated with offering banking services to a particular customer, and its capacity and systems to effectively manage those risks. It is not the Board's policy to discourage banking organizations from offering services to any class of law-abiding financial services consumers or businesses.

Payment Services Offered by Nonbanks

Many of the questions that have arisen with respect to the customer due-diligence expectations of the federal banking agencies relate to the involvement of nonbanks as intermediaries or providers of financial services, including money services businesses (MSBs) and third-party payment processors (TPPPs). MSBs provide financial services, such as check cashing, money remittance, and other services, to customers that do not have traditional bank accounts. Some MSBs include large, globally active companies while others are small businesses such as gas stations and convenience stores offering financial products and services. By comparison, TPPPs are bank customers that provide payment-processing services to merchants and other entities such as telemarketers and online businesses. Both MSBs and TPPPs engage in transactions with individuals and companies who are not direct customers of the bank.

The Federal Reserve follows guidance issued in 2005 by the federal banking agencies and the Financial Crimes Enforcement Network (FinCEN) governing account relationships with

MSBs.[5] That guidance confirms that banking organizations may provide banking services to MSBs that operate lawfully. The guidance is intended to assist banks in the decision to open and maintain accounts for legitimate businesses by identifying the programs and procedures they should have in place to perform customer due diligence and monitoring of these customers for suspicious activity.

The Federal Reserve also follows the interagency examination manual and related guidance issued by FinCEN when evaluating the procedures banking organizations use to manage account relationships with TPPPs.[6] These entities often use their commercial bank accounts to conduct payment processing for their merchant clients. The guidance is designed to assist banking organizations in designing and implementing policies and systems for monitoring and managing the risks associated with the payment and lending products they offer. The objective of the guidance and the Federal Reserve's supervisory activities is to direct banking organizations to take appropriate steps to offer their services to legitimate and law-abiding customers, and to minimize the risk of facilitating money laundering, terrorist financing, or other illicit activity.

Examination and Enforcement Process

In 1986, Congress included in the Money Laundering Control Act the requirement that the Federal Reserve and other federal banking agencies examine the AML program and procedures banking organizations use to assure compliance with the BSA and report problems

---

[5] See Financial Crimes Enforcement Network, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision (2005), "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States" (April 26).

[6] See *infra* note 4 at pp. 239-242. See also Financial Crimes Enforcement Network (2012) "Risk Associated with Third-Party Payment Processors" (October 22).

with a bank's procedures to management. Under the Money Laundering Control Act, the federal banking agencies are required to take formal, public action against a financial institution that fails to establish and maintain the required program or correct problems with the program that were previously reported to the institution by the supervisors.

Consistent with this mandate, the Federal Reserve generally conducts regular on-site examinations of each bank it is charged with supervising on an alternating basis with state banking supervisors. As part of these examinations, examiners review the institution's AML procedures and its compliance with the BSA. For large, complex banking organizations, the safety and soundness examination process is continuous, and anti-money-laundering and BSA compliance is incorporated into the examination process.

When we find that a bank has not adopted a program and procedures that properly meet the bank's BSA obligations, the matter is discussed with bank management and noted in the institution's report of examination. The Federal Reserve's enforcement actions under the BSA typically are aimed at correcting deficiencies in an organization's policies and procedures for monitoring account activities and identifying unlawful or suspicious transactions.

Recent Justice Department Initiative

Finally, regarding the focus of this hearing, Operation Choke Point is an initiative of the Department of Justice and not an initiative of the Federal Reserve. The Department of Justice has the sole authority to indict or seek criminal fines or other sanctions and to criminally prosecute individuals and businesses for their actions. As we have testified previously, the Federal Reserve cooperates with other agencies in various enforcement actions, including by

providing information in response to subpoenas issued by the Justice Department or other federal law enforcement authorities.[7]

Thank you very much for inviting me to present the Federal Reserve's views on these important issues. I would be pleased to answer any questions you may have.

[7] "Patterns of Abuse: Assessing Bank Secrecy Act Compliance and Enforcement": Hearing before the S. Comm. on Banking, Housing and Urban Affairs, 113th Congress (2013) (statement of Jerome H. Powell, Governor, Board of Governors of the Federal Reserve System).

Department of Justice

STATEMENT

OF

STUART F. DELERY
ASSISTANT ATTORNEY GENERAL
CIVIL DIVISION

BEFORE THE
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

FOR A HEARING RELATED TO

"OPERATION CHOKE POINT"

PRESENTED ON

JULY 15, 2014

Statement of Stuart F. Delery
Assistant Attorney General, Civil Division
Before the U.S. House of Representatives
Committee on Financial Services
Subcommittee on Oversight and Investigations
July 15, 2014

Chairman McHenry, Ranking Member Green, and Members of the Subcommittee, thank you for inviting me here and for providing the Department of Justice the opportunity to appear at today's hearing to describe our work designed to protect consumers from fraud perpetrated by certain merchants, third-party payment processors, and banks.

As the Attorney General has said, the Justice Department has made it a priority to fight consumer fraud of all kinds and to hold the perpetrators accountable. Consumer fraud comes in many forms—from telemarketing fraud to mortgage fraud, from lottery scams to predatory and deceptive on-line lending—and often strips our most vulnerable citizens of their savings and even their homes.

While there is seemingly no limit to the kinds of schemes that perpetrators of fraud invent, many of these schemes have one thing in common: they employ the banking system to take money from their victims. Once a fraudulent merchant can work his way into the banking system, he no longer has to convince unwitting consumers to hand over cash or mail a check. Instead, with the click of a button, he can debit their bank accounts and credit his own, repeatedly, without permission, and in violation of federal law—until somebody does something to stop it.

The Civil Division's Consumer Protection Branch—along with the Criminal Division and United States Attorney's Offices across the country—has worked for decades to protect the health, safety, and economic security of the American consumer. Based on its years of experience in combating fraudulent merchants, the Department, along with our law enforcement and regulatory partners, recognizes the critical role played by a limited number of third-party payment processors—intermediaries between banks and merchants—in allowing fraudulent merchants to gain access to our banking system and consumers' bank accounts. In some cases, these payment processors open bank accounts in their own names and, for a fee, use these accounts to conduct banking activities on behalf of their customers. While some customers are legitimate businesses, others are fraudulent merchants who either choose not to open their own bank accounts or cannot do so because banks will not do business with them. At the merchants' direction, the processor will initiate debit transactions against consumers' accounts and transmit the money to the fraudulent merchant.

Guided by the facts and the law, and by following the flow of money from fraudulent transactions, the Department has learned that some third-party payment processors know their merchant clients are engaged in fraud and yet continue to process

their transactions—in violation of federal law. Further, our experience in these cases has been that some banks, in violation of the law, either know about the fraud they are facilitating or are consciously choosing to look the other way. As a result, in November 2012, our attorneys proposed a concentrated effort to pursue the fraud committed by the banks and payment processors. This strategy aims both to hold accountable those banks and processors who violate the law and to prevent access to the banking system by the many fraudulent merchants who had come to rely on the conscious assistance of banks and processors in facilitating their schemes. This effort is sometimes referenced as Operation Chokepoint.

To begin the effort, using a variety of public and nonpublic sources, the Consumer Protection Branch assembled evidence of fraudulent activity by specific fraudulent merchants, payment processors, and banks. That information included statements of cooperating witnesses; tips and referrals from defrauded consumers and banks whose customers had been victimized; and evidence obtained during investigations of fraudulent merchants that identified third-party payment processors or banks participating in the merchants' unlawful conduct.

In addition, we obtained information from the Federal Reserve Bank of Atlanta concerning banks with abnormally high "return rates"—one possible indicator of potential fraud. "Return" or "chargeback" rates refer to the percentage of transactions that are reversed. In addition to "unauthorized" returns, which represent an explicit claim that a consumer did not authorize a debit in a transaction account, a high rate of "total" returns also indicates potential fraud. For example, returns due to insufficient funds may reflect consumers who had money taken from their accounts unexpectedly or repeatedly, without authorization. Returns due to a closed account may reflect consumers who were forced to close their bank accounts as a consequence of unauthorized debits.

Based on these and other sources, between February and August 2013, the Consumer Protection Branch issued civil subpoenas to specific banks, processors, and other entities for which the Department had specific evidence suggesting that those entities might be engaged in fraud or might have evidence of fraudulent conduct by others. We then reviewed the information provided in response to those subpoenas and, depending upon the nature of the evidence, we sought additional information, determined to pursue a civil or criminal investigation, or closed the file.

One of those investigations now has been resolved, and its resolution demonstrates exactly the type of troubling relationship between a bank and a set of perpetrators of fraud that gave rise to the Department's effort. On April 25, 2014, the U.S. District Court for the Eastern District of North Carolina entered a consent order and approved a settlement agreed to by the Department and Four Oaks Bank. According to the Department's complaint, Four Oaks allowed a third-party payment processor to facilitate payments for fraudulent merchants despite active and specific notice of the fraud, including:

- Four Oaks received hundreds of notices from consumers' banks—submitted under penalty of perjury—that the people whose accounts were being charged had not authorized the debits from their accounts.

- Four Oaks had evidence that more than a dozen merchants served by the payment processor had a "return rate" over 30 percent—a strong sign the bank was facilitating repeated fraudulent withdrawals. Indeed, one merchant had a return rate of over 70 percent.

- Four Oaks had evidence of efforts by merchants to conceal their true identities.

According to the Department's complaint, despite these and many other signals of fraud, Four Oaks permitted the third-party payment processor to originate approximately $2.4 billion in debit transactions against consumers' bank accounts, for which the bank received more than $850,000 in fees. As a result of the bank's actions, many American consumers were defrauded of their hard-earned savings.

The consent order, agreed to by Four Oaks and approved by the court, requires Four Oaks Bank to pay $1 million to the U.S. Treasury as a civil monetary penalty and to forfeit $200,000 to the U.S. Postal Inspection Service's Consumer Fraud Fund. It also obligates Four Oaks to take steps to prevent future consumer fraud.

As the Four Oaks Bank case demonstrates, the Department's policy is to base its investigations on specific evidence of unlawful conduct. Nevertheless, in recent months, we have become aware of reports suggesting that these efforts instead represented an attack on businesses engaged in lawful activity. I thank you for this opportunity to clear up this misconception. Our policy is to investigate specific conduct, based on evidence that consumers are being defrauded—not to target whole industries or businesses acting lawfully, and to follow the facts wherever they lead us, in accordance with the law, regardless of the type of business involved. We think this endeavor demonstrates the importance of holding financial institutions accountable when they participate in fraudulent activities, just as we hold accountable any other entity that engages in unlawful conduct.

As with virtually all of our law enforcement work that touches upon highly regulated industries, our work in this area includes communication with relevant regulatory agencies, here including the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and the Federal Reserve Board. Such communication is designed to ensure that we understand the industry at issue, that our investigations do not unnecessarily or improperly frustrate regulatory efforts, and that we have all the information needed to evaluate the enforcement options available to address violations that our investigations uncover.

Federal law requires banks to "know their customers" in a variety of ways and to report instances of suspicious activity in order to prevent money laundering, consumer

fraud, and other illegal behavior. Banks are aware of these laws, and most have instituted programs to comply with these longstanding requirements. Indeed, it is because of these programs that many fraudulent merchants have difficulty engaging directly with banks and have come to rely on third-party payment processors for access to the banking system. Noting this trend, the FDIC—as part of its regulatory responsibilities—has warned banks about the heightened risks to consumers associated with third-party payment processors in its Guidance on Payment Processor Relationships first issued in 2008, and has explained that, "[a]lthough many clients of payment processors are reputable merchants, an increasing number are not and should be considered 'high risk.'" The FDIC has provided examples of "high-risk merchants" for purposes relevant to its regulatory mission. The Department's mission is to fight fraud, and we recognize that an entity's simply doing business with a merchant considered "high risk" is not fraud.

Indeed, we recognize that most of the businesses that use the banking system—even those in industries considered "high risk"—are not engaged in fraud, and we are dedicated to ensuring that our efforts to combat fraud do not discourage or inhibit the lawful conduct of honest merchants. While the Department's complaint against Four Oaks Bank demonstrates that many of the fraudulent merchants for which Four Oaks provided access to the banking system were engaged in illegal online short-term lending, we follow the facts where they lead us. The Department would only be interested in the conduct of an online short-term lender, or any merchant, to the extent that its conduct violates the law.

I thank you for this opportunity to reiterate what I and other Department officials have made clear on numerous occasions: that the Department is seeking to protect consumers from fraudulent practices in all industries and has no interest in pursuing or discouraging businesses engaged in lawful conduct. The Attorney General said this in a recent video posted publicly on the Department website. The Department has said this in response to Congressional inquiries. And the Department has said this many times to industry groups, including in a letter I wrote to the American Bankers Association and the Electronic Transaction Association.

Our efforts to protect consumers by pursuing fraudulent banking activity are not focused on financial institutions that merely fail to live up to their regulatory obligations or that unwittingly process a transaction for a fraudulent merchant. We are fighting fraud. When a bank either knows or is willfully ignorant to the fact that law-breaking merchants are taking money out of consumers' bank accounts without valid authorization, and the bank continues to allow that to happen, that is not just a concern for bank regulators. That is fraud, and it can result in true devastation for consumers. When any entity—whether it is a merchant, a third-party payment processor, or a bank—commits fraud against consumers, the Department will not hesitate to enforce the law. We will continue to pursue our mission to protect honest, hardworking Americans from those who put their financial security in peril.

Thank you, once again, for the opportunity to appear before you today. At this time, Mr. Chairman, I would be happy to address any questions you or Members of the Subcommittee may have.

STATEMENT OF

FEDERAL DEPOSIT INSURANCE CORPORATION

by

RICHARD J. OSTERMAN, JR.
ACTING GENERAL COUNSEL

on

SUPERVISION OF BANKS' RELATIONSHIPS WITH THIRD PARTY PAYMENT PROCESSORS

before the

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
COMMITTEE ON FINANCIAL SERVICES
U.S. HOUSE OF REPRESENTATIVES

July 15, 2014
2128 Rayburn House Office Building

Chairman McHenry, Ranking Member Green and members of the Subcommittee, I appreciate the opportunity to testify on behalf of the Federal Deposit Insurance Corporation (FDIC) on the FDIC's supervisory approach regarding insured institutions establishing account relationships with third-party payment processors (TPPPs). I also will discuss the FDIC's interaction with the Department of Justice's consumer fraud initiative, Operation Choke Point.

As the primary federal regulator of state-chartered financial institutions that are not members of the Federal Reserve System, the FDIC is responsible for supervising these institutions for adherence with safety and soundness standards, information technology requirements, Bank Secrecy Act and other anti-money laundering laws and regulations, and consumer protection laws[1].

The USA PATRIOT Act, enacted in 2001, added new due diligence requirements for banks under the Bank Secrecy Act (BSA). Section 326 of the Act requires banks to establish and maintain a Customer Identification Program (CIP). At a minimum, financial institutions must implement reasonable procedures for: (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency. The purpose of the CIP is to enable banks to form a reasonable belief that they know the true identity of each customer. In its most basic form, knowing one's customer serves to protect banks from

[1] For state-chartered financial institutions that are not members of the Federal Reserve System with assets of more than $10 billion, the FDIC and the Consumer Financial Protection Bureau each have supervisory authority pursuant to certain consumer protection laws.

the potential liability and risk of providing financial services to an unscrupulous customer. In addition, but no less important, it provides another level of protection to the general public against illegal activity (including terrorist financing and money laundering) since banks are a common gateway to the financial system.

Certain kinds of businesses, transactions, or geographic locations may pose greater risk for suspicious or illegal activity. Higher-risk activities have been understood by industry[2] and the financial regulators as activities that may be subject to complex or varying legal and regulatory environments, such as activities that may: be legal only in certain states; be prohibited for certain consumers, such as minors; be subject to varying state and federal licensing and reporting regimes; or tend to display a higher incidence of consumer complaints, returns, or chargebacks. Because these risks may be posed directly by a bank's customer, or indirectly through relationships established by bank customers with other parties (merchants, for example), banks have enhanced their customer due diligence policies and processes to better protect against harm. Harm to the bank can range from operating losses attributable to unanticipated consumer reimbursements that were not properly reserved for, to civil or criminal actions for facilitation of violations of law.

As challenging as it can be for financial institutions to understand the risks involved in the activities of a direct customer, the difficulty is magnified when the activities involve third parties. TPPPs may have relationships with hundreds or even thousands of merchant clients for

[2] https://www.paypal.com/us/webapps/mpp/ua/acceptableuse-full
https://payments.amazon.com/help/Amazon-Simple-Pay/User-Agreement-Policies/Acceptable-Use-Policy
https://support.google.com/wallet/business/answer/75724

which they initiate transactions. The vast majority of transactions passing through financial institutions and payment processors are legitimate transactions initiated by reputable merchants. These functions provide a valuable service to customers, both individual consumers and businesses, and are typically performed at a low cost. For example, banks often process customers' automated clearing house (ACH) transactions to credit or debit a bank account of another party as a service for their customers.

However, where transactions from the merchant client of a bank's TPPP customer are not legitimate, there is real risk for the bank because it can be held legally responsible for facilitating the activities and transactions of the TPPP. This is because in cases where the transaction was initiated by a third party, the bank still has a relationship, albeit indirect, with the TPPP's merchant clients, and thus would be exposed to the risks associated with their transactions. If the bank, through its customer relationship with the TPPP, is facilitating activity that is either impermissible in a state or being performed in a manner illegal under applicable state or federal law, the bank can be exposed to significant risks. As a financial regulator, the FDIC is responsible for ensuring that the financial institutions we supervise fully appreciate these risks, have policies and procedures in place to identify and monitor these risks, and take reasonable measures to manage and address these risks.

Supervisory Approach

Traditionally, TPPPs contracted primarily with U.S. retailers that had physical locations in the United States to help collect monies owed by customers on the retailers' transactions.

These merchant transactions primarily included credit card payments, but also covered ACH and remotely created checks (RCCs). Guidance for FDIC-supervised institutions conducting business with TPPPs was contained within examination manuals and guidance related to credit card examinations, retail payment systems operations, and the Bank Secrecy Act.[3] However, as the financial services market has become more complex, the individual federal banking agencies, the Federal Financial Institution Examinations Council (FFIEC) and the Financial Crimes Enforcement Network (FinCEN) have issued additional guidance on several occasions warning financial institutions of emerging risks and suggesting mitigation techniques.

In December 2007, the Federal Trade Commission and seven state attorneys general initiated lawsuits against payment processors who processed more than $200 million in debits to consumers' bank accounts on behalf of fraudulent telemarketers and Internet-based merchants.[4] In April 2008, an insured financial institution that provided account relationships to payment processors whose merchant clients experienced high rates of return for unauthorized transactions or customer complaints of failure to receive adequate consideration in the transaction was fined a $10 million civil money penalty by its regulator. The penalty documents note that the institution failed to conduct suitable due diligence even though it had reason to know that the payment

[3] See FDIC Credit Card Activities Manual, http://www.fdic.gov/regulations/examinations/credit_card/index.html, June 12, 2007; FFIEC Retail Payment Systems Handbook, http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems.aspx, February 25, 2010, (update to March, 2004 release); and, Federal Reserve, SR-93-64 (FIS), Interagency Advisory, Credit Card-Related Merchant Activities, http://www.federalreserve.gov/boarddocs/srletters/1993/SR9364.HTM, November 18, 1993; Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm, April 29, 2010 (most recent update to original June 30, 2005 release).

[4] See FTC Press Release, December 11, 2007, *FTC and Seven States Sue Payment Processor that Allegedly Took Millions form Consumers Bank Accounts on Behalf of Fraudulent Telemarketers and Internet-based Merchants.*

processors were customers that posed significant risk to the institution.[5] The Office of the Comptroller of the Currency and FDIC subsequently issued guidance that described the risks associated with TPPPs processing ACH and RCC for higher-risk merchants.[6] In 2010, the FFIEC updated the Retail Payment Systems Handbook to provide expanded guidance on merchant card processing and ACH and RCC transactions. The update provided a more in-depth discussion of the increased risks posed by these activities and some of the risk management tools that financial institutions can use to mitigate them.[7]

In late 2010 and through 2011, the FDIC observed TPPPs servicing disreputable merchants seeking to do business with small, troubled institutions.[8] This led the FDIC to issue expanded guidance in January 2012. In October 2012, FinCEN issued an Advisory noting that law enforcement had reported that recent increases in certain criminal activity had demonstrated that TPPPs presented a risk to the payment system by making it vulnerable to money laundering, identity theft, fraud schemes and illicit activity.[9]

---

[5] See United States of America, Department of the Treasury, Comptroller of the Currency, AA-EC-08-13, In the Matter of: Wachovia Bank, National Association, Charlotte, North Carolina, Consent Order for a Civil Money Penalty.

[6] FDIC Financial Institution Letter, FIL-44-2008, *Guidance for Managing Third-Party Risk*, issued June 2008; and FDIC Financial Institution Letter, FIL-127-2008, *Guidance on Payment Processor Relationships*, issued November 2008.

[7] FFIEC, Retail Payment Systems Booklet, http://www.ffiec.gov/press/pr022510.htm.

[8] See Consent Agreement between the FDIC and SunFirst Bank, St. George, Utah, dated November 9, 2010 (FDIC-I0-845b); Notice of Assessment issued by the FDIC in the matter of Fist Bank of Delaware, Wilmington, Delaware, dated November 16, 2012 (FDIC-12-306k); FTC Press Release, FTC Charges Massive Internet Enterprise with Scamming Consumers Out of Millions Billing Month-After-Month for Products and Services They Never Ordered, http://www.ftc.gov/news-events/press-releases/2010/12/ftc-charges-massive-internet-enterprise-scamming-consumers-out, December 22, 2010; FTC Press Release, FTC Action Bans Payment Processor from Using a Novel Payment Method to Debit Accounts, http://www.ftc.gov/news-events/press-releases/2012/01/ftc-action-bans-payment-processor-using-novel-payment-method, January 5, 2012; FTC Press Release, Defendants Banned from Payment Processing, Will Pay $950,000 in FTC Settlement, http://www.ftc.gov/news-events/press-releases/2013/03/defendants-banned-payment-processing-will-pay-950000-ftc, March 13, 2013.

[9] FDIC Financial Institution Letter, FIL-3-2012, *Payment Processor Relationships, Revised Guidance*, issued January 2012; and Department of the Treasury FinCEN Advisory, FIN-2012-A010, *Risk Associated with Third-Party Payment Processors*, issued October 2012.

A review of the relationships between banks and their customers or TPPPs is a regular component of the FDIC's examination process. Our supervisory approach focuses on assessing whether financial institutions are adequately overseeing activities and transactions they process and appropriately managing and mitigating related risks. Our supervisory efforts to communicate these risks to banks are intended to ensure that institutions perform the due diligence, underwriting and ongoing monitoring necessary to mitigate the risks to their institutions.

Where an institution is following the regulatory guidance and properly managing its account relationships with TPPPs, the institution has not been criticized. When we find that an institution is not properly managing its account relationships with TPPPs, the matter is discussed with bank management and noted in the institution's report of examination. If the deficiencies are not addressed, the bank may become the subject of an enforcement action to effect corrective action.

Most recently, in September of last year, the FDIC issued a Financial Institution Letter that clarifies and reminds financial institutions of the FDIC's policy and supervisory approach.[10] It states that financial institutions that properly manage relationships and effectively mitigate risks are neither prohibited nor discouraged from providing payment processing services to customers, regardless of the customers' business models, provided they are operating in compliance with applicable state and federal law. The FDIC re-emphasized this policy to address any confusion that may have existed about our supervisory approach, and we have

[10] Financial Institution Letter, FIL-43-2013, *FDIC Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities*, issued September 2013.

reiterated this policy to our bank supervision managers and examiners to ensure that examiners are following this policy.

In recent years, FDIC-supervised banks have heard from a number of state and federal agencies regarding the importance of ensuring that banks are properly managing their relationships with certain customers and third party payment processors. A number of states have expressed concerns about banks facilitating activities, especially online, that are illegal in their states. At the federal level, the Department of Justice (DOJ) also has actively contacted banks about similar issues. When the concerns and actions have involved FDIC-supervised institutions, the FDIC has cooperated with law enforcement and state regulators.

In early 2013, the FDIC became aware that DOJ was conducting an investigation into the use of banks and third party payment processors to facilitate illegal and fraudulent activities. From the FDIC's perspective, DOJ's efforts were aimed at addressing potential illegal activity being processed through banks. To the extent that the DOJ's actions were directed at potential illegal activity involving the banks that we supervise, the FDIC has a responsibility to consider the legality of certain actions involving our institutions as well as any potential risks such activities could pose for institutions we regulate.

The FDIC frequently coordinates with other agencies -- both federal and state -- in its supervision of our regulated institutions. Accordingly, FDIC staff communicated and cooperated with DOJ staff involved in Operation Choke Point based on an interest in DOJ's investigation into potential illegal activity that may involve FDIC-supervised institutions. FDIC attorneys'

communication and cooperation with DOJ included requests for information about the investigation, discussions of legal theories and the application of banking laws, and the review of documents involving FDIC-supervised institutions obtained by DOJ in the course of its investigation. At all times, these attorneys worked for the FDIC and were performing their duties as lawyers for the FDIC in furtherance of the FDIC's mission.

In conclusion, the FDIC's supervisory approach focuses on assessing whether financial institutions are adequately overseeing activities and transactions they process and appropriately managing and mitigating related risks. Our supervisory efforts to communicate these risks to banks are intended to ensure institutions perform the due diligence, underwriting, and monitoring necessary to mitigate the risks to their institutions.

The FDIC does not and should not make business decisions for the banks that we supervise. Indeed, each bank must decide the persons and entities with which it wants to have a customer or business relationship. The FDIC has stated very clearly and publicly that financial institutions that properly manage customer relationships and effectively mitigate risks are neither prohibited nor discouraged from providing payment processing services to customers, regardless of the customers' business models, provided they are operating in compliance with applicable state and federal law.

Thank you and I am happy to take any questions.

For Release Upon Delivery
10:00 a.m., July 15, 2014

TESTIMONY OF

DANIEL P. STIPANO

DEPUTY CHIEF COUNSEL

OFFICE OF THE COMPTROLLER OF THE CURRENCY

Before the

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

HOUSE COMMITTEE ON FINANCIAL SERVICES

UNITED STATES HOUSE OF REPRESENTATIVES

July 15, 2014

Statement Required by 12 U.S.C. § 250:
The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

Introduction

Chairman McHenry, Ranking Member Green, and members of the Subcommittee, I have been invited to testify today as the Subcommittee reviews the Department of Justice's (DOJ's) Operation Choke Point investigation.

As the Deputy Chief Counsel for the Office of the Comptroller of the Currency, I have worked on Bank Secrecy Act and anti-money laundering issues for over 20 years. In my position, I represent the OCC on the Treasury Department's Bank Secrecy Act Advisory Group and the National Interagency Bank Fraud Working Group. Throughout my career, I have witnessed many cases where banks have been used, wittingly or unwittingly, as vehicles for fraud, terrorist financing, money laundering, and other illicit activities. Deterring such abuses is an important objective of our examination work and of the supervisory guidance we provide to bankers.

I appreciate having this opportunity to discuss how the OCC works to ensure that the institutions we supervise comply with federal laws and regulations, including the Bank Secrecy Act (BSA). However, the OCC is not part of Operation Choke Point and therefore my testimony will focus on the OCC's supervisory policies and actions.

It is OCC's policy to cooperate with law enforcement investigations and the OCC routinely receives and processes requests for information from law enforcement agencies. When not prohibited by law, the OCC provides other federal agencies, including the DOJ, with bank examination reports and other non-public OCC information when such information is requested by, and necessary for, those agencies to perform their official duties. Some of the official requests for examination reports and other non-public information the OCC received from DOJ during 2013 related to Operation Choke Point.

OCC Supervision

The OCC's primary mission is to charter, regulate, and supervise national banks, federal savings associations, and the federal branches and agencies of foreign banks. In carrying out this mission, the OCC requires banks to soundly manage their risks, meet the needs of their communities, comply with laws and regulations, and provide fair access to financial services and fair treatment of their customers.

Banking institutions – large and small – play a crucial role in providing consumers and businesses across the nation with essential financial services and sources of credit that are critical to economic growth and job expansion. The safety and soundness of an institution can be threatened when a bank lacks appropriate risk management systems and controls for the products or activities it provides or the customers it serves. These controls are critical to ensure that our financial institutions are not used to perpetrate fraud, money laundering, terrorist financing, or other forms of illicit activity.

Currently there is great concern that banks are terminating the accounts of entire categories of customers, without regard to the bank's ability to manage the risks posed by those customers, and some have suggested that regulators are dictating those actions. As a general matter, the OCC does not recommend or encourage banks to engage in the wholesale termination of categories of customer accounts. Rather, we expect banks to assess the risks posed by individual customers on a case-by-case basis and to implement appropriate controls to manage each relationship. The Comptroller reiterated this message last March in a speech to the Association of Certified Anti-Money Laundering Specialists when he stated, "no matter what type of business you are dealing with, you

have to exercise some sound judgment, conduct your due diligence, and evaluate customers individually."[1]

This is consistent with the approach the OCC takes in enforcing compliance with the BSA. The BSA and its implementing regulations require financial institutions to have systems and controls to appropriately monitor accounts for potential criminal violations and suspicious activity indicative of money laundering or terrorist financing. If we find significant weaknesses in a bank's systems and controls, we will require the bank to take appropriate corrective action. In more serious cases, we will require corrections through an enforcement action. In rare cases where a customer has engaged in suspected criminal or other illegal activity, or the bank cannot properly manage the risk of an activity, we may order the bank through an enforcement action to terminate the customer's account.

While we require banks to put appropriate controls in place to prudently manage their risks, outside of the enforcement context, the ultimate decision of whether to open, close, or maintain an account rests with the bank. In some cases, the bank may determine that it cannot effectively manage the risks on a cost-effective basis, and decide to close the account or exit a line of business. These are business decisions made by the bank itself and not dictated by the OCC. In fact, many banks have policies that call for them to close accounts based on certain criteria, such as after a certain number of Suspicious Activity Reports have been filed in connection with a customer, and we expect banks to comply with their own policies.

---

[1] Remarks by Comptroller Curry before the Association of Certified Anti-Money Laundering Specialists on March 17 available at http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-39.pdf

Payment Processors

The OCC recognizes the need for banks to provide services for a variety of customers, consistent with their business plans, and has issued bulletins on a wide range of topics to provide helpful guidance and best practices for banks to follow. For example, since the early 1990's the OCC has had in place principles for risk management for banks that maintain accounts for payment processors. These principles are embodied in guidance we issued in 2006,[2] which we subsequently updated in 2008[3] in connection with an OCC enforcement action against Wachovia Bank.[4] The OCC took this enforcement action in response to significant deficiencies in the bank's oversight of its business relationships with certain of its payment processor customers. Our 2008 updated guidance addressed the need for banks to have effective due diligence, underwriting, and monitoring systems in place for payment processors that are bank customers.

The Wachovia action is an example of the consequences a bank can face if it fails to implement proper controls to monitor and manage the risks posed by a customer's account. In this case, the OCC found that Wachovia failed to properly oversee the activity of third-party payment processor accounts despite significant red flags indicating consumers were being harmed by telemarketers that were the payment processors' customers. Many of the telemarketers deliberately targeted vulnerable populations, such as the elderly, using deceptive, high-pressure sales calls to convince these consumers to provide their personal checking account information to purchase products of dubious or

---

[2] OCC Bulletin 2006-39, "Automated Clearing House Activities - Risk Management Guidance," http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html

[3] OCC Bulletin 2008-12, "Payment Processors - Risk Management Guidance," http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html

[4] Formal Agreement, Wachovia Bank, N.A., Charlotte, North Carolina, and the Office of the Comptroller of the Currency, AA-EC-08-12 (April 24, 2008) and Consent Order for a Civil Money Penalty, Wachovia Bank, N.A., North Carolina, and the Office of the Comptroller of the Currency, AA-EC-08-13 (April 24, 2008).

no value. Payment processors used consumers' account information to create checks that were deposited into telemarketers' accounts at the bank. Because the consumers never received what the telemarketers promised, or funds were taken from their accounts without proper authorization, the bank received hundreds of complaints and hundreds of thousands of the checks created by the payment processors were returned to the bank.

Despite these significant red flags, and having clear knowledge that consumers were being harmed, the bank failed to properly address the situation. The OCC cited the bank for unsafe or unsound practices as well as unfair practices in violation of section 5 of the Federal Trade Commission Act, required it to pay approximately $144 million in fines and restitution to consumers, and ordered other affirmative relief. The OCC did not require the bank to cease doing business with any third-party payment processors or telemarketers. Rather, the OCC's action was focused on requiring the bank to remediate specific consumer harm and establish enhanced risk management policies, procedures, systems, and controls to mitigate the risk of future harm to consumers.

Money Services Businesses

Press reports have indicated that banks have been terminating relationships with accounts of Money Services Businesses (MSBs). For banks that choose to open or maintain accounts for MSBs, the OCC has long taken the position that banks should apply the requirements of the BSA based on their assessment of risk, as they do for all customers, taking into account the products and services offered as well as any individual circumstances. Nine years ago, the Federal banking agencies and the Financial Crimes Enforcement Network (FinCEN) issued guidance clarifying our compliance expectations

for providing banking services to MSBs.[5] The guidance set forth our supervisory expectations for compliance with the requirements of the BSA and applicable state law.

Depending on its activities, an MSB can be considered a high-risk customer of a bank. The BSA requires financial institutions to conduct appropriate due diligence and review account documentation for all customers to determine whether the activity in these accounts is consistent with the customer's business or occupation and the stated purpose of the account. The purpose of these requirements is to ensure that the bank is not used to perpetrate money laundering, terrorist financing, or other illicit activity. Some financial institutions recently have elected not to offer accounts to high-risk MSB customers because of the costs associated with monitoring these accounts and ensuring compliance with the BSA. However, it is important to note that nothing in the BSA prohibits a financial institution from providing accounts to MSBs, even high-risk MSBs, as long as the institution's systems and controls are sufficient to effectively monitor the activity in these accounts.

Conclusion

As a general matter, the OCC does not direct banks to open, close, or maintain accounts. Those are business decisions the bank must make for itself. But we require banks to put controls in place to manage the risks posed by their accounts. We recognize that banks need to make judgments about their risk tolerances and how they manage and control each customer relationship. Our reviews of a bank's controls are a matter of supervisory judgment. If the bar is set too high, it can cause a bank to terminate accounts of legitimate businesses. However, if the bar is set too low, the consequences can be dire,

[5] Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses operating in the United States, issued April 26, 2005; http://www.fincen.gov/statutes_regs/guidance/html/guidance04262005.html

allowing the bank to be used as a vehicle to facilitate fraud, money laundering, terrorist financing, or other forms of illicit finance. Such activities can jeopardize the safety and soundness and even the viability of an institution. Consequently, we strive for a supervisory approach that is reasonable, balanced, and fair, and results in systems and controls that are effective in preventing and deterring the use of our nation's financial institutions for illicit purposes.

THE DEPARTMENT OF JUSTICE'S "OPERATION CHOKE POINT"

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON FINANCIAL SERVICES SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

July 15, 2014

Dear Chairman and Ranking Member:

My name is Marsha Jones, and I am the President of the Third Party Payment Processors Association (TPPPA). I am pleased to provide testimony on behalf of the organization and the industry.

Third-party payment processing is an integral part of the payments industry and the economy as a whole. Payment processors are the technology innovators that provide consumers faster and easier ways to make payments, and provide small and mid-sized businesses an opportunity to collect and make payments electronically. This enables them to compete more effectively in a global marketplace with their larger competitors. Third party payment processors also provide direct deposit of payroll, providing consumers with safe and immediate access to their paycheck.

A third party payment processor (TPPP) is a depository customer of a bank that processes payments on behalf of other companies (merchants) through the TPPP's banking relationship. The role of the TPPP is to provide merchants with access to the electronic payments system, so that the merchants' customers have the ability to make electronic payments to the merchant and the merchant can make electronic payments to employees (direct deposit of payroll) and their business partners (business-to-business payments.) Third party payment processors typically have hundreds of customers that they process for including, mom-and-pop grocery stores, day-care centers, homeowner associations and more. They also provide access to, and payment and technical support for tens of thousands of merchants for which payment processing directly through a bank would be cost prohibitive.

The most vulnerable of small businesses rely on third party payment processors to enable them to participate in electronic payments, as they may not meet the standards to set up direct payment processing services through a bank directly. For example, they may be too small to qualify to process payments through a bank, they are too new, or they are struggling to turn their company around and no longer meet the credit requirements of a bank to process payments. This category has grown significantly since the financial crisis. These are the primary business beneficiaries of third party payment processing.

Consumers rely upon third party payment processors for virtually all direct deposit of payroll, most innovative mobile payment solutions and many of the bills and online purchases that they make. Third party payment processors provide consumers with more electronic payment choices than credit cards. These expanded choices have become increasingly more important as consumers' access to credit has decreased, providing the opportunity for some vulnerable consumers, without access to credit cards, to continue to make electronic payments.

Like other financial institutions, third party payment processors seek a diverse portfolio of customers to help manage risk. If a payment processor elects to process for higher-risk merchants, the typical payment processor diversifies their payments portfolio with some higher risk and low risk transactions. This protects the processor and the bank from credit risk. However, the processor still has contractual and regulatory due diligence obligations that it has to meet with regards to these high risk merchants.

This third party role has become the subject of significant scrutiny by banking regulators and by the Justice Department, and appears to be the genesis of Operation Choke Point. Unfortunately, however, what appears to have started as a legitimate interest in targeting a few companies who may have facilitated fraudulent transactions has morphed into a significant attack on the whole industry. The impact of Operation Choke Point has been significant not only on the third party payment processors, and on the targeted, high-risk, and lawful industries that it seeks to disrupt, but also on the low-risk merchants that our members serve, as well as the consumers that benefit from the payment services.

Operation Choke Point is designed to sever the flow of funds to target merchants by separating either the processor or merchant from the banking system. However, when a processor is shut off from the banking system, ALL of their merchants are disrupted, including those for small businesses and direct deposit of payroll for consumers, resulting in harm to the economy and harm to consumers.

The strategy of Operation Choke Point causes severe collateral damage. Targeting a merchant by going after a payment processor that processes a wide variety of payments to businesses of all types as well as consumer payroll has far-reaching and devastating impact.

The Third Party Payment Processors Association is fully supportive of prosecuting merchants or processors who engage in or perpetuate fraud against consumers. However, we strongly believe Operation Choke Point has resulted in casting too wide a net and is an irresponsible and ineffective strategy.

The TPPPA recognizes that we have a responsibility to help our bank and processor members, and merchants they serve, to comply with the applicable laws and regulations. As such, we are voluntarily creating an industry best practices system as a means of self-regulating the third party payment processing industry. This Compliance Management System (CMS) will help enable banks and third party payment processors, as well as merchants to comply with the laws and regulation and ensure that proper due diligence is performed throughout the third payment processing system. We believe that this is the most responsible and effective way to impact change without disrupting innovation, hurting small businesses and robbing consumers of effective and innovative ways of making and receiving payments.

We thank the House Financial Services Committee for holding this important hearing and for the opportunity to present our written testimony.

"The hallmark of the TPPPA is promoting compliance as the road to achieve payments integrity and excellence." Marsha Jones, President, Third Party Payment Processors Association (TPPPA)

THIRD PARTY PAYMENT PROCESSOR ASSOCIATION (TPPPA)

The TPPPA is a national not-for-profit industry association representing and promoting the interests of payment and payroll processors, their financial institutions and their merchants. The TPPPA formed in the summer of 2013 to raise awareness of the unintended consequences of Operation Choke Point and to create industry best practices in compliance for third party payment processing.

The TPPPA was formed to address the unmet needs of payment processors and their financial institutions that primarily process Automated Clearing House (ACH) and remotely created checks (RCC) payments.

TPPPA Leadership

- President

Marsha Jones, AAP, NCP

- Board of Directors

Intercept (Fargo, ND)
Repay (Atlanta, GA)
ACHWorks (Gold River, CA)
EFT Network (Hawthorne, NY)
Secure Payments Systems (San Diego, CA)

President's Bio

- Accredited ACH Professional (AAP)
- National Check Professional (NCP)
- 6 years at Viewpointe Regional Payments Association (NACHA)

Member of NACHA's Risk Management & Advisory Group
Created and Facilitated Third-Party Sender Roundtable
Designed ACH Originator Compliance Self Assessment

- 7 years at Capitol Bancorp Ltd

Responsible for all payments processing for 50+ Community Banks

- 7 years at Wells Fargo Bank

Operations Manager Small Business Lending Renewal Team

Our Mission

In service of our members and the payments industry our mission is to provide:

- *Advocacy*
- *Leadership*
- *Support*

Advocacy

TPPPA advocates on behalf of its members as to the vital role processors play in our economy. Promoting and representing the interests of our members, and forging productive relationships with:

- Members of Congress
- Regulators
- Rule-Making Bodies (NACHA, ECCHO)
- Other trade associations, (ABA, ICBA, ETA, Regional Payment Associations)

Leadership

TPPPA provides leadership in the industry by working with stakeholders to explore opportunities and examine solutions to innovate in a compliant manner.

- Create industry best practices through our Compliance Management System.
- Engage members and industry stakeholders in the payments rulemaking.

Support

All TPPPA members receive exclusive and ongoing training, guidance and compliance support.

- Processor and Financial Institution members receive the Compliance Management System (CMS) as part of their membership at no additional cost.
- TPPPA supports other trade associations in their payments compliance efforts.

Code of Conduct

The Third Party Payment Processors Association is a not-for profit trade association responsible for providing advocacy, support and industry leadership to its members. The Association has adopted a Code of Conduct to ensure the activities that affect the payments industry and its members are conducted with the highest levels of integrity, professionalism and fairness. All active members of the Association will subscribe to the following Code of Conduct:

1. *Adhere to the spirit as well as the letter of all applicable regulations, rules and laws related to the payments it processes.*
2. *Avoid even the appearance of professional misconduct or criminal offense.*
3. *Conduct business in a manner that does not adversely impact the membership or the payments industry.*
4. *Conduct all activities in a professional and businesslike manner.*
5. *Remain current on financial obligations to Association.*
6. *Respect the privacy and confidentiality of the membership and member business.*

The Association reserves the right to disassociate itself from any organization that, in its opinion, fails to abide by our Code of Conduct.

Members Categories:

- Members (Voting and Non-Voting)
    - Payment Processors
    - Payroll Processors
    - Financial Institutions
- Affiliate Members (Non-Voting)
    - Merchants
    - Vendors
    - Other Associations
    - Other Industry Stakeholders

The TPPPA Compliance Management System

Policies that are tailored to the unique needs and responsibilities of TPPPA members:
Payment and Payroll Processors
Financial Institutions

Created to address the oversight of relevant regulatory agencies, including FDIC, OCC, FRB, CFPB and FinCEN

Processor Module
Written for payment and payroll processors policies incorporate guidance for:

- Due diligence and enhanced due diligence
- Ongoing monitoring, management and review
- Detecting and reporting suspicious activity

Policies include:

- BSA/AML/OFAC
- Consumer Complaints
- UDAAP
- Information Security, Privacy, Red Flags
- High Risk Verticals
- Telemarketing, Debt Collections, Lending
- And more

Financial Institution Module
Written for FIs with processors as customers. Helps incorporate existing policies of the financial institution into a cohesive program for third party payment processing.

Both Modules Address

- Risk Assessment (Due Diligence and Underwriting)
- Agreements
- Merchant Training
- Ongoing Monitoring
- Periodic Review
- Escalation and Reporting Suspicious Activity
- Termination of Merchant Relationships

Regulator Interaction and Relationships

The TPPPA has conducted meetings with the following regulators to introduce them to the TPPPA and to socialize our Compliance Management System methodology:

Commission of State Bank Supervisors (CSBS)
Consumer Financial Protection Bureau (CFPB)
Federal Trade Commission (FTC)
Federal Depository Insurance Corporation (FDIC)
Office of the Comptroller of the Currency (OCC)
Federal Reserve Bank (FRB)

These meetings were productive and the following objectives were met:

- Introduced the association, our mission, purpose and immediate objectives
- Created an open dialog with regulatory agencies
- Created framework for sharing the TPPPA's CMS and receiving feedback

TPPPA's Commitment to the CMS

The TPPPA is committed to reviewing and updating the CMS on an ongoing basis to ensure alignment with changes to regulation, regulatory guidance and payment system rule changes. We are committed to continual improvement of the policy set and will add new policies as needed. For example, a policy for Remotely Created Checks and a policy for Managing Cross Channel is slated for the 2015 release. We are also committed to vetting the CMS with regulators and rule making bodies on an ongoing basis. The TPPPA will provide regulators with an initial copy of the CMS by August, 2104.

CMS Certification for Payment Processors

The TPPPA is in the process of developing control framework for a voluntary SSAE16 Certification Audit with an independent audit firm. Successful completion of a SOC1 audit in year one and SOC2 thereafter, will make processor eligible for certification by the association. The TPPPA CMS Certification Audit is estimated to be available in September 2014.

CMS Consulting and Training

The TPPPA provides consulting and training to assist members in integrating the CMS policies into their payments practices. We recognize policies alone do not make a difference unless they are used to align practices, processes and procedures with CMS policies, and have the policies drive the company culture and behavior. Ongoing training and support will be made available to the members to support the association's compliance objectives.

Contact Us:

Third Party Payments Processors Association (TPPPA)
20 F Street NW, 7th Floor
Washington, DC 20001
www.tpppa.org
Marsha Jones, AAP, NCP
President
(602) 402-0416 – Cell
mjones@tpppa.org

Pots of marijuana cash cause security concerns

Trevor Hughes, USATODAY 12:50 p.m. EDT July 13, 2014

(Photo: Matthew Staver for USA TODAY)

DENVER — The unmarked armored truck rumbles to a stop in a narrow alley, and former U.S. Marine Matthew Karr slides out, one hand holding a folder, the other hovering near the pistol holstered at his hip.

With efficient motions he retrieves a locked, leather-bound satchel from a safe set into the truck's side and presses a buzzer outside the door. It swings open to reveal a cavernous warehouse filled with marijuana and a safe stuffed with cash.

Welcome to the rear guard of Colorado's rapidly expanding legal marijuana industry, where eager users pour millions of dollars — most of it in small bills — into buying pot, hashish, and marijuana-infused foods and drinks. All that cash adds up, and there are few places to put it: Federal regulations, which still classify pot as an illegal drug, make it difficult for marijuana producers to deposit their profits into traditional bank accounts.

And those cash-heavy small businesses make awfully attractive — and vulnerable — targets for criminals.

That's where Karr and the company he works for come in.

Heading through the warehouse where workers tend young marijuana plants, Karr greets a young woman, and the two empty a safe of tens of thousands of dollars in cash neatly packed in plastic envelopes. Like every room in this combined marijuana store and grow house, the smell of pot hangs heavy in the air. Karr double-checks the ledger, locks his satchel and hustles outside, where former cop Phil Baca waits at the wheel of the armored car.

Karr opens the truck's safe, pitches the satchel inside and climbs back into the passenger seat, an AR-15 rifle stashed behind him. It's a scene that plays out six times in three hours. Their take for the day: somewhere close to $100,000 in cash.

"For the first three months, people were just keeping the money everywhere — in the walls, in mattresses, at home," says Sean Campbell, CEO of Blue Line Protection Group, which provides marijuana security services, including Karr, Baca and the armored car. "And banks don't even want to deal with it. You have a quarter-of-a-million dollars in cash show up all at once. The counting time alone is going to take an hour."

The unusual problem of having too much cash is forcing business owners to hire security firms like Campbell's, especially after Denver police warned in June of a credible threat against marijuana stores and couriers.

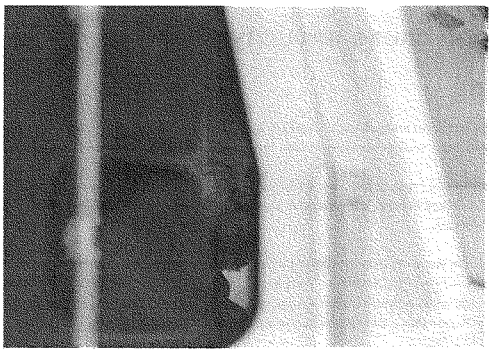
Marijuana-store owners have suffered some smash-and-grab robberies over the last several years but surveillance systems and close police attention have solved many of them. Experts say those robberies were largely committed by amateurs, rather than sophisticated crime rings.

Campbell said he believes it will take a serious high-dollar heist to force smaller marijuana stores to take their security more seriously.

State law requires marijuana businesses to have security cameras and systems on the premises, and many have armed guards, but they remain easy targets. The stores and grow operations often are in remote industrial areas, in warehouses that have not been hardened against a determined intruder. Many stores have large amounts of pot sitting around in rooms secured only by flimsy wooden doors.

Options are limited, however. Unlike most other businesses, marijuana-store owners can't easily open bank accounts for fear of running afoul of federal law. Despite Washington state joining Colorado last week in legalizing sales of marijuana for recreational purposes and 23 states plus the District of Columbia permitting medical pot, the federal government still classifies the plant as an illegal drug more dangerous than cocaine or methamphetamine.

By opening a bank account, pot growers and shop owners run the risk of being charged with money laundering, because federal banking laws and regulations are deliberately aimed at tracking large flows of cash like those generated by both legal and illegal drug sales. A single such charge can bring decades in prison, and most banks and pot-shop owners don't want to run that risk.



Matt Karr waits in the armored car as Philip Baca (not pictured) makes a delivery. *(Photo: Matthew Staver for USA TODAY)*

"When you go into the business, and you know it's federally illegal, you're taking your chances," said Tom Gorman, who runs the federally funded Rocky Mountain High Intensity Drug Trafficking Area task force. "That's the problem when the state legalizes something that remains illegal at the federal level."

While declining to be quoted by name, many marijuana store owners interviewed by USA TODAY shared tales of playing cat-and-mouse with banks, managing to keep accounts open for only a few months at a time before getting shut down.

U.S. Treasury officials require banks to file what are known as "suspicious activity reports" whenever they suspect someone is trying to launder money. Anyone bringing in a pile of cash sets off internal alarms for bank workers, pot-shop workers say. Federal financial-crimes investigators encourage banks to report suspected marijuana transactions because pot remains illegal at the federal level.

"Our goal is to promote financial transparency and make sure law enforcement receives the reporting from financial institutions that it needs to police this activity and to make it less likely that this financial activity will run underground and be much harder to track," said Steve Hudak, a spokesman for the Treasury Department's Financial Crimes Enforcement Network.

Tax-and-marijuana attorney Rachel Gillette said she's seen banks' concerns firsthand — several banks she deals with said they wouldn't let her open an account, even though both the federal and state government are allowed to deposit tax payments from pot sellers. Gillette said federally regulated banks say it's just easier for them not to risk getting their hands tainted by pot.

"They literally told me they would not take my account because I do business with the marijuana industry," Gillette said. "That seems fundamentally unfair — the state is taking that money and putting it in the bank; the IRS is taking that money and putting it in the bank."

Philip Baca checks off each smaller bag of marijuana from an inventory list.*(Photo: Matthew Staver for USA TODAY)*

Gillette is suing the IRS on behalf of one of her clients who has been paying federal payroll tax bills with cash. The IRS calls for electronic payments and adds a 10% surcharge for cash payments, she said. With some marijuana businesses paying payroll taxes of $100,000 a quarter, those penalties are substantial.

Colorado has tried to solve the problem with a new state law permitting creation of marijuana banking cooperatives, which would have the power to accept deposits, lend money and make electronic payments. But that system likely won't begin operating for at least another year, said Gov. John Hickenlooper, and even then federal officials would need to bless the plan.

The amount of cash already flowing through the fast-growing system has forced state tax officials to change how they accommodate payments. While Colorado allows businesses to pay their taxes in cash, most pay electronically. Marijuana businesses, however, must trek to a central Denver office, cash in hand, where they're met at the curb by armed guards and escorted inside.

"Some people walk in with shoe boxes. Some people have it in locked briefcases. We've had people bring it in buckets," said Natriece Bryant, a spokeswoman for the Colorado Department of Revenue.

Campbell, who runs the armored-car company, said the vast cash flows are a clear come-on for criminals. He said he's working with banks to offer alternatives for marijuana businesses, including vault services. For many in the marijuana industry, the scene from the Emmy-winning television series *Breaking Bad* of a storage unit filled with drug cash hits uncomfortably close to reality.

Says Campbell, "You're effectively creating a magnet for crime."

Read or Share this story: http://usat.ly/1m6UvqZ

Questions for the Record from
Rep. Blaine Luetkemeyer (MO-3)
Committee on Financial Services
U.S. House of Representatives

"The Department of Justice's 'Operation Choke Point'"
Subcommittee on Oversight and Investigations
July 15, 2014

Questions to Stuart Delery, Assistant Attorney General, U.S. Department of Justice

1. **During your appearance before this Committee, you indicated that the Department of Justice (DOJ) had no participation in the creation of heightened scrutiny lists used by the Federal Deposit Insurance Corporation (FDIC) or other banking regulators. Please confirm that DOJ had no role in the creation of any FDIC heightened scrutiny list or any similar list created by another federal regulator.**

   The Department of Justice was not to my knowledge involved in the creation of the FDIC list of examples of merchant categories that was contained within any FDIC guidance, or any similar list. It is my understanding that the FDIC has since removed that list from its guidance to eliminate any misconceptions about FDIC policy.

2. **You indicated during your testimony before this Committee that DOJ had not utilized in any way a list of industries designated as deserving heightened scrutiny by the FDIC. Yet a DOJ subpoena entered into the record of a July 17th hearing in the House Committee on the Judiciary included such a list. Please clarify your statement to this Committee and indicate whether or not DOJ has ever utilized in any way a heightened scrutiny list produced by a federal banking regulator, included but not limited to the FDIC.**

   During the hearing before this Committee, I was asked by Chairman McHenry whether the Department of Justice created the FDIC list of examples of merchant categories, and I responded that the list was not a DOJ list. I also indicated in my testimony that the Department is not interested in targeting any particular lawful industry and that the mere fact that an entity provides services to a business in an industry that appears on a regulator's list was not the basis for any of the subpoenas I authorized.

   As has been discussed publicly, the majority of the subpoenas that the Department of Justice issued to financial institutions as part of the investigations at issue included, as an enclosure, regulatory guidance from the FDIC, the Office of the Comptroller of the Currency, and the Financial Crimes Enforcement Network. These guidance documents were included to give context for the subpoenas. They describe how fraudulent merchants use the payment system, advise banks about the money laundering and fraud risks associated with providing banking services through third-party payment processors, and describe how banks can assist law enforcement by recognizing and reporting

fraudulent activity. Within the seven-page FDIC guidance, there is a footnote that includes examples of merchant categories that "may pose elevated risk."

As I said during my testimony, at no time was this list a basis for the issuance of a subpoena or the initiation of an investigation by the Department. I and other Department officials have made clear publicly that our policy is to investigate specific unlawful conduct, based on evidence that consumers are being defrauded – not to target whole industries or businesses acting lawfully.

When have such lists been used by DOJ? Was such a list attached in every subpoena issued as a result (either formally or informally) of Operation Choke Point? Have such lists been used by DOJ in any other way?

As I stated in response to the previous question, at no time was the FDIC list, or any other similar list, a basis for the issuance of a subpoena or the initiation of an investigation by the Department.

FDIC guidance, along with the guidance of other industry regulators, was included with the majority of subpoenas issued by the Department. As noted, this guidance contained FDIC's list of merchant categories in a footnote. I am unaware that the FDIC list has been cited or used by the Department in any other way. It is my understanding that the FDIC has since removed that list from its guidance to eliminate any misconceptions about FDIC policy.

Response to Questions
from the Honorable Blaine Luetkemeyer
by the Federal Deposit Insurance Corporation

Q1: During your testimony you indicated that heightened scrutiny lists are created based on experience of banking regulators and other factors including but not limited to consumer complaints and previous indications of fraud. Please provide a detailed explanation of how exactly these heightened scrutiny lists are created. More specifically, please provide all information that led to the creation of the heightened scrutiny list used in the September 17, 2013, presentation by Michael Benardo, Division of Risk Management Supervision, to the Federal Financial Institutions Examination Council.

A1: The FDIC has not created "heightened scrutiny lists." The FDIC included examples of telemarketing or Internet merchant categories that have been associated with higher-risk activity in financial institution guidance[1] and an informational article[2] on the potential risks associated with third-party payment processor (TPPP) relationships. These examples included activities that could be subject to complex or varying legal and regulatory environments, such as those that may be legal only in certain states; those that may be prohibited for certain consumers, such as minors; those that may be subject to varying state and federal licensing and reporting regimes; and those that may result in higher levels of complaints, returns, or chargebacks.

The examples cited in previous guidance and the informational article were drawn from the payments industry itself. The major credit card networks, such as Visa and MasterCard, use merchant codes as a mechanism for identifying merchant types and business lines and to designate higher-risk industries that require increased due diligence and fraud monitoring. Other national payment providers, such as PayPal, use similar systems for identifying increased risk in payments.[3] These designations are not static, as industries are added or removed based on experience.

The examples of merchant categories associated with higher-risk activity used by Michael Benardo during a Federal Financial Institutions Examination Council (FFIEC) training presentation on September 17, 2013, were a subset of the examples included in the informational article.

On July 28, 2014, the FDIC issued a Financial Institution Letter[4] that clarifies our supervisory approach to institutions establishing account relationships with TPPPs and removed the examples of merchant categories from previously published guidance and the informational article. The examples were intended to be illustrative of trends identified by the payments industry at the time the guidance and article were released and, therefore, considered to be incidental to the primary purpose of the

---

[1] FIL 127-2008, "Guidance on Payment Processor Relationships," http://www.fdic.gov/news/news/financial/2008/fil08127.html, FIL-3-2012, "Payment Processor Relationships, Revised Guidance," http://www.fdic.gov/news/news/financial/2012/fil12003.html, and FIL-43-2013, "FDIC Supervisory Approach to Payment Processing Relationships with Merchant Customers That Engage in Higher-Risk Activities," http://www.fdic.gov/news/news/financial/2013/fil13043.html.

[2] "Managing Risks in Third-Party Payment Processor Relationships," *Supervisory Insights*, Summer 2011.

[3] https://www.paypal.com/us/webapps/mpp/ua/acceptableuse-full
https://payments.amazon.com/help/Amazon-Simple-Pay/User-Agreement-Policies/Acceptable-Use-Policy
https://support.google.com/wallet/business/answer/75724

[4] FIL-41-2014, "FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors," http://www.fdic.gov/news/news/financial/2014/fil14041.html.

guidance. However, the examples of merchant categories have led to misunderstandings regarding the FDIC's supervisory approach to institutions' relationships with TPPPs, resulting in the misperception that the listed examples of merchant categories were prohibited or discouraged. It is the FDIC's policy that insured institutions that properly manage customer relationships are neither prohibited nor discouraged from providing services to customers operating in compliance with applicable federal and state law. Accordingly, as part of clarifying our guidance, the FDIC removed the examples of merchant categories from outstanding guidance and the article.

Q2: Please provide all information that led to the inclusion of "firearms/fireworks sales" on the list used in the aforementioned September 17, 2013 presentation.

A2: The inclusion of "firearms/fireworks sales" as examples of merchant categories that have been associated with higher-risk activity as part of the September 17, 2013 FFIEC training conference presentation and in the informational article titled, "Managing Risks in Third-Party Payment Processor Relationships," was based on what the payments industry considered, at that time, to be higher-risk industries requiring increased due diligence and fraud monitoring. These industries are examples of activities that could be subject to complex or varying legal and regulatory environments, such as those that may be legal only in certain states or cities; those that may be prohibited for certain consumers, such as minors and certain convicted felons that may be seeking anonymity on the Internet; and those that may be subject to varying state and federal licensing and reporting regimes.

Q3: We know of two lists naming industries that the Federal Deposit Insurance Corporation (FDIC) views as meriting heightened scrutiny. How many FDIC heightened scrutiny lists exist? Please provide a copy of each list created and/or used by FDIC staff to designation industries that merit heightened scrutiny.

A3: The FDIC does not maintain "heightened scrutiny lists." The examples of merchant categories that have been associated with higher-risk activity cited in previous guidance, the informational article, and at internal training presentations were intended to inform institutions about industries that may be subject to complex or varying legal and regulatory environments and those that may result in higher levels of complaints, returns, or chargebacks. The examples were not intended to prevent institutions from maintaining relationships with particular industries. As previously stated, these examples were drawn from the payments industry. As noted in response to question 1, the FDIC issued a FIL on July 28, 2014,[5] to clarify our supervisory approach to institutions establishing account relationships with TPPPs and removed the examples of merchant categories from previously issued guidance and the informational article.

Q4: What is the process for sharing FDIC heightened scrutiny lists with other federal agencies, including but not limited to the Department of Justice (DOJ)? When did FDIC staff first share heightened scrutiny lists with DOJ staff? More specifically, when and in what manner was the heightened scrutiny list presented on September 17, 2013, first shared with DOJ?

---

[5] FIL-41-2014, "FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors," http://www.fdic.gov/news/news/financial/2014/fil14041.html.

A4: As discussed previously, the FDIC does not maintain "heightened scrutiny lists," and therefore there is no process for sharing them with other federal agencies or DOJ. The examples of merchant categories that have been associated with higher-risk activity were first made publicly available in an informational article titled, "Managing Risks in Third-Party Payment Processor Relationships" published in the FDIC's Supervisory Insights, Summer 2011 issue. A subset of those examples, which were drawn from the payments industry, also was included in a January 2012 FIL.[6] With regard to the September 17, 2013 presentation, during a Federal Financial Institutions Examination Council training conference, the examples of merchant categories associated with higher-risk activities were used in a slide by FDIC staff during a panel discussion where FDIC, OCC, and DOJ staff each made presentations about TPPPs. The slide deck used in the presentation may have been shared with conference organizers and/or other participants in advance of the presentation.

On July 28, 2014, the FDIC issued a Financial Institution Letter[7] that clarifies our supervisory approach to institutions establishing account relationships with TPPPs and removed the examples of merchant categories from previously published guidance and the informational article. The examples were intended to be illustrative of trends identified by the payments industry at the time the guidance and article were released and, therefore, considered to be incidental to the primary purpose of the guidance.

---

[6] FIL-3-2012, "Payment Processor Relationships, Revised Guidance," http://www.fdic.gov/news/news/financial/2012/fil12003.html

[7] FIL-41-2014, "FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors," http://www.fdic.gov/news/news/financial/2014/fil14041.html.

Questions for Scott G. Alvarez, General Counsel, Board of Governors of the Federal Reserve System from Representative Maloney:

1. I appreciate that the Federal Reserve has sought to tailor its capital requirements generally, and has chosen to apply its Supplementary Leverage Ratio (SLR) to only a subset of U.S. banks. However, even within that subset, there are crucial differences business models that may make the SLR appropriate as a back-up tool for some banks, but less useful for others. For example, regulation for the same large global universal bank with significant retail and trading activities may not be appropriate for a bank that is not engaged in trading, investment banking, and consumer activities. Is the Fed factoring in the riskiness of the business model and balance sheet as it is crafting the SLR?

In 2013, the Federal Reserve Board, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency (the Agencies) adopted revisions to their capital rules to strengthen the capital requirements applicable to banking organizations.[1] These revisions included a minimum supplementary leverage ratio (SLR) requirement of 3 percent for banking organizations subject to the Agencies' advanced approaches rules. The SLR is measured as the ratio of tier 1 capital to a banking organization's total leverage exposure, which is equal to a measure of the banking organization's total assets plus its off-balance sheet exposures.[2] On September 3, 2014, the Agencies adopted a final rule modifying the definition of the measure of total leverage exposure (the denominator of the SLR) to better measure the amount of certain on- and off-balance sheet exposures. In adopting this rule, the Agencies considered comments requesting that it exclude certain low-risk assets from the measure of total leverage exposure.

The purpose of the SLR is to require a banking organization to hold a minimum amount of capital against total assets and off-balance sheet exposures, regardless of the riskiness of the individual assets. In this way, the SLR serves as a complement to the agencies' risk-based capital requirements, which take into account the riskiness of a banking organization's assets and off-balance sheet exposures. Consistent with the purpose of the SLR, the agencies did not exempt or limit any categories of on-balance sheet assets from the denominator of the SLR.

---

[1] 78 FR 55340 (interim final rule) (September 10, 2013) (FDIC) and 78 FR 62018 (October 11, 2013) (OCC and Board). On April 8, 2014, the FDIC adopted as final the interim final rule, with no substantive changes.

[2] Banking organization is subject to the advanced approaches rule if it has consolidated assets of at least $250 billion, if it has total consolidated on-balance sheet foreign exposures of at least $10 billion, if it elects to apply the advanced approaches rule, or it is a subsidiary of a depository institution, bank holding company, or savings and loan holding company that uses the advanced approaches to calculate risk-weighted assets. See 78 FR 62018, 62204 (October 11, 2013); 78 FR 55340, 55523 (September 10, 2013).